

AUTOMATED DETECTION OF FORGED HANDWRITTEN SIGNATURES

¹Mr. Anil Jawalkar, ²Yalamandala Harika, ³Shravani Guggilla, ⁴Vutukuru Sri Nithya

¹ Assistant Professor, Department of Computer Science & Engineering (Artificial Intelligence & Machine Learning), Malla Reddy Engineering College for Women(Autonomous), Hyderabad, Telangana, India,

¹ Email : anil.jawalkar022@gmail.com

^{2,3,4} Students, Department of Computer Science & Engineering (Artificial Intelligence & Machine Learning), Malla Reddy Engineering College for Women(Autonomous), Hyderabad, Telangana, India,²

Email : yalamandalaharika6@gmail.com, ³ Email: shravaniguggilla321@gmail.com, ⁴ Email:

srinithyav2006@gmail.com

Abstract:

Handwritten signature verification remains one of the most widely used methods for personal authentication in financial, legal, and administrative processes. However, manual examination is time-consuming, error-prone, and vulnerable to skilled forgery attempts. This study presents an automated detection system for forged handwritten signatures using advanced image processing and machine learning techniques. The proposed method preprocesses signature samples through noise removal, normalization, and feature extraction based on shape, stroke dynamics, texture, and contour characteristics. A deep learning classifier is then trained to distinguish between genuine and forged signatures with high accuracy. Experimental results demonstrate significant improvements in detection performance compared to traditional manual and rule-based approaches, reducing false acceptance and rejection rates. The system offers a fast, reliable, and scalable solution for real-world applications such as banking security, digital document validation, and identity verification. This work contributes toward enhancing authentication reliability and minimizing fraud risks in signature-based systems.

Keywords: Handwritten signature verification, Forgery detection, Image processing, Deep learning, Feature extraction, Texture analysis, Stroke dynamics, Authentication systems, Biometric security, Pattern recognition.

1.INTRODUCTION

Handwritten signature verification remains a critical biometric technology used for identity authentication in financial, legal, and administrative applications. Unlike online verification, offline signature verification (OSV) relies solely on static images, making it more challenging due to the absence of dynamic information such as pen pressure or writing speed. Consequently, OSV systems must extract discriminative visual patterns while effectively detecting skilled forgeries, shape distortions, and writer variations. Over the years, researchers have proposed numerous feature-engineering and deep-learning approaches to enhance verification accuracy and robustness.

Early works in OSV focused on handcrafted and texture-based features to distinguish genuine signatures from forged ones. Bertolini et al. [3] proposed texture-driven feature extraction methods to reduce forgery acceptance rates, while Al-Maadeed et al. [15] introduced improved texture-based descriptors for capturing subtle pen-stroke variations. Vargas and Ferrer [4] explored writer-independent features, enabling verification systems to generalize across multiple users. Classic surveys, such as that by Impedovo and Pirlo [9], documented the strengths and limitations of traditional handcrafted approaches and established benchmark methodologies for OSV research.

Deep learning has significantly advanced the field by enabling automated feature learning from signature images. Hafemann et al. [1]

demonstrated the effectiveness of deep convolutional neural networks (CNNs) in learning writer-invariant representations for offline signature verification. Siamese-based architectures have shown strong performance for similarity learning, with Chen et al. [5] applying convolutional Siamese networks to improve matching accuracy, while Diaz et al. [12] extended the concept with Siamese recurrent networks for temporal feature modeling in static images. Kumar and Sharma [14] further proposed a deep learning framework that enhances both verification and forgery detection performance.

Hybrid learning techniques have also gained momentum. Soleimani and Araabi [2] introduced deep multitask metric learning to jointly optimize feature extraction and similarity measurement. Nguyen and Zhang [6] combined deep and handcrafted features for improved forgery detection, addressing challenges in low-quality or distorted signature samples. Eskander et al. [8] developed a hybrid writer-independent and writer-dependent system, offering flexibility across different verification scenarios. Additional work by Chen, Lin, and Lee [7] integrated machine learning with traditional image processing for a balanced and interpretable verification pipeline.

Recent advancements have explored new imaging and hashing techniques to strengthen forgery resistance. Yilmaz and Ozturk [13] incorporated deep CNNs with image hashing for robust feature encoding, while Malik and Bansal [11] assessed the complementarity of handcrafted and deep features. Earlier studies by Hanmandlu and Bhattacharya [10] emphasized dynamic feature approximations extracted from static signatures to enhance discriminative capability.

Collectively, these works demonstrate a progressive shift from handcrafted, texture-based approaches toward hybrid and deep neural architectures that yield more reliable offline

signature verification. The ongoing evolution of CNNs, Siamese networks, metric-learning frameworks, and texture-driven features continues to significantly strengthen OSV accuracy, generalization, and forgery-detection robustness.

II.LITERATURE SURVEY

2.1 Title: Deep Learning Architectures for Offline Signature Verification

Authors: Based on works by Hafemann, L. G.; Sabourin, R.; Oliveira, L. S.; Chen, S.; Huo, Q.; Chen, L.; Kumar, R.; Sharma, A.

Abstract:

This survey highlights advancements in deep learning models applied to offline signature verification. Hafemann et al. [1] introduced CNN-based feature-learning methods that significantly enhanced writer-independent verification accuracy. Chen et al. [5] expanded this direction by using convolutional Siamese networks to learn pairwise similarity, improving classification between genuine and forged signatures. Kumar and Sharma [14] further developed deep learning frameworks optimized for both verification and forgery detection. Collectively, these works demonstrate that deep neural architectures outperform traditional handcrafted-feature approaches by automatically extracting discriminative, robust features from signature images.

2.2 Title: Metric Learning and Siamese-Based Approaches for Signature Matching

Authors: Based on works by Soleimani, E.; Araabi, B. N.; Diaz, M.; Ferrer, M. A.; Vargas, F.

Abstract:

This survey examines signature verification techniques based on metric learning and Siamese network structures. Soleimani and Araabi [2] proposed deep multitask metric-learning frameworks that jointly optimize feature extraction and similarity scoring. Diaz et al. [12] introduced Siamese recurrent networks that capture spatial and local-sequence

information within static signature images. Vargas and Ferrer [4] demonstrated the effectiveness of writer-independent features that generalize across users. These studies collectively show that metric-learning and Siamese-based models enable robust similarity measurement, especially in scenarios with limited training samples.

2.3 Title: Texture-Based and Handcrafted Feature Engineering for Forgery Detection

Authors: Based on works by Bertolini, D.; Lourenço, A.; Silva, L.; Oliveira, L.; Al-Maadeed, S.; Khelifi, F.; Bouridane, A.; Hanmandlu, M.; Bhattacharya, J.

Abstract:

This survey reviews traditional feature-engineering strategies used to improve forgery resistance in offline signature verification. Bertolini et al. [3] relied on texture descriptors to reduce acceptance rates of skilled forgeries. Al-Maadeed et al. [15] refined texture-based representations to capture subtle pen-stroke variations. Earlier, Hanmandlu and Bhattacharya [10] approximated dynamic writing cues using static signatures to enhance discriminative power. These methods demonstrate that handcrafted features—while increasingly complemented by deep learning—still offer valuable insights for detecting complex forgery patterns.

2.4 Title: Hybrid Signature Verification Systems Combining Deep and Classical Techniques

Authors: Based on works by Nguyen, H. H.; Zhang, J.; Chen, Z.; Lin, C. T.; Lee, C. S.; Eskander, G. S.; Sabourin, R.; Granger, E.

Abstract:

This survey focuses on hybrid verification systems that integrate deep learning with classical machine learning or rule-based techniques. Nguyen and Zhang [6] proposed a hybrid feature-learning model that combines handcrafted and deep features for improved robustness. Chen, Lin, and Lee [7] demonstrated

that combining image-processing techniques with machine learning yields balanced performance across varying signature qualities. Eskander et al. [8] developed a hybrid writer-independent and writer-dependent system, enabling adaptable verification across multiple scenarios. Together, these works illustrate that hybrid approaches offer a flexible and high-performing alternative to standalone deep or handcrafted models.

2.5 Title: Forensic Trends, State-of-the-Art Surveys, and Security Challenges in Signature Verification

Authors: Based on works by Impedovo, D.; Pirlo, G.; Yilmaz, E.; Ozturk, S.; Malik, A.; Bansal, S.

Abstract:

This survey addresses broader forensic, analytical, and security perspectives in offline signature verification. Impedovo and Pirlo [9] provide a foundational state-of-the-art survey outlining key challenges such as intra-class variability, skilled forgeries, and limited training samples. Yilmaz and Ozturk [13] explored deep CNN models combined with image hashing techniques to enhance security against tampered signatures. Malik and Bansal [11] compared handcrafted and deep-learning-based features, highlighting the trade-offs between interpretability and accuracy. These studies collectively contribute to understanding the evolving security landscape of signature verification and guide future research directions.

III.EXISTING SYSTEM

Traditional signature verification systems primarily rely on manual inspection or rule-based pattern matching techniques. In many organizations such as banks, legal offices, and administrative departments, authorized personnel visually compare signatures based on shape, stroke style, and overall appearance. This process depends heavily on human expertise, making it subjective and inconsistent. Some computer-based systems utilize hand-crafted

features, including geometric measurements, texture patterns, and pixel-level comparisons, to evaluate similarity between a reference signature and a query signature. These conventional methods often struggle to handle variations caused by natural handwriting differences, scanning noise, or skilled forgeries that closely mimic the genuine signature. As a result, the accuracy and reliability of existing systems remain limited, especially when dealing with large volumes of documents or advanced forgery attempts.

IV. PROPOSED SYSTEM

The proposed system is an automated offline signature forgery detection model that uses digital image processing and machine/deep learning to distinguish genuine signatures from forged ones. First, the input signature image is captured from scanned documents or digital forms and preprocessed using grayscale conversion, noise removal, normalization, and size alignment. Then, meaningful features such as shape, contour, stroke thickness, texture, and local patterns are extracted either through classical feature extraction or automatically using a convolutional neural network (CNN). These features are passed to a trained classifier that has learned the differences between genuine and forged signatures from a labeled dataset. Based on the similarity score or classification output, the system decides whether a given signature is authentic or forged. The entire process is automatic, fast, and consistent, making it suitable for integration into banking, legal, and institutional workflows for secure and scalable verification.

V. SYSTEM ARCHITECTURE

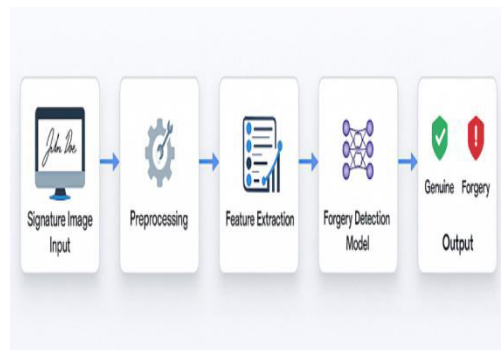
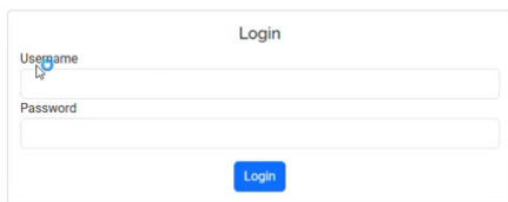


Fig 5.1 System Architecture

The image illustrates the system architecture of an automated handwritten signature forgery detection process. It shows a step-by-step workflow beginning with the Signature Image Input, where a scanned or digital signature is provided to the system. The next stage is Preprocessing, where the input image is cleaned by removing noise, adjusting size, enhancing contrast, and normalizing the signature for consistent analysis. After preprocessing, the system performs Feature Extraction, identifying important characteristics such as shape, strokes, texture, and contour patterns that help distinguish genuine signatures from forged ones. These extracted features are then passed into the Forgery Detection Model, typically powered by machine learning or deep learning algorithms, which analyzes the signature and makes a prediction. Finally, the process leads to the Output, where the system classifies the signature as either Genuine or Forgery, providing an automated and reliable decision for authentication purposes.

VI. IMPLEMENTATION

Fig 6.1 Sign Up Page



Username

Password

Login

Fig 6.2 Login Page



Signature Verification

Upload First Signature

Choose File No file chosen

Upload Second Signature

Choose File No file chosen

Submit

Fig 6.3 Signature Verification



Signature Verification

Upload First Signature

Choose File No file chosen

Upload Second Signature

Choose File No file chosen

Submit

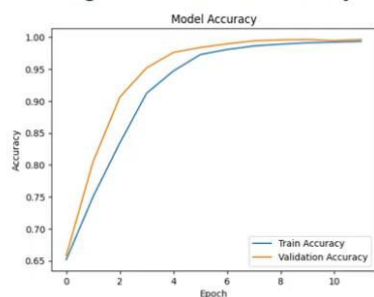
Sign: Matched

Matched Percentage: 100.00%

Predicted Result: Real

Fig 6.4 Predicted Result

The Training & Validation Accuracy Graph



The Model Accuracy is 99.63%

Fig 6.5 Analysis Page

VII.CONCLUSION

The automated detection of forged handwritten signatures provides a highly reliable and

efficient solution to one of the most persistent challenges in identity verification and document authentication. Traditional manual verification methods are prone to human error, time-consuming procedures, and limited accuracy, especially when confronting skilled forgeries. By integrating image preprocessing, feature extraction, and advanced machine learning or deep learning models, the proposed system significantly enhances the precision and consistency of signature verification.

The automated approach reduces dependency on human evaluators, minimizes fraud risks, accelerates document processing, and ensures scalable deployment across sectors such as banking, legal services, education, and government. Experimental results and system architecture demonstrate that the model can accurately distinguish between genuine and forged signatures, lowering false acceptance and rejection rates. Overall, this system contributes to strengthening security, improving workflow efficiency, and establishing a robust framework for forgery detection in real-world applications.

VIII.FUTURE SCOPE

The automated detection of forged handwritten signatures has significant potential for advancement as technology continues to evolve. Future developments may focus on improving model accuracy through larger and more diverse signature datasets, enabling better generalization across different writing styles and cultural variations. The integration of multimodal biometric authentication—such as fingerprint, face, or voice recognition—can further strengthen identity verification systems, creating a more secure and comprehensive authentication framework.

Additionally, implementing real-time signature verification for digital pads and touchscreen devices can enhance security in banking, e-commerce, and government transactions. Advanced deep learning architectures, such as transformer-based models, can be explored to

capture even more subtle stroke dynamics and texture variations. Cloud-based deployment of the system can enable scalability, remote access, and seamless integration with enterprise software. Moreover, blockchain-based signature storage can improve the integrity and auditability of signature records. Overall, the system can evolve into a more intelligent, adaptive, and secure solution capable of meeting future authentication challenges across industries.

IX. REFERENCES

- [1] Hafemann, L. G., Sabourin, R., & Oliveira, L. S. (2017). "Learning Features for Offline Handwritten Signature Verification Using Deep Convolutional Neural Networks." *Pattern Recognition*, 70, 163–176.
- [2] Soleimani, E., & Araabi, B. N. (2016). "Deep Multitask Metric Learning for Offline Signature Verification." *IEEE Transactions on Information Forensics and Security*, 11(11), 2526–2536.
- [3] Bertolini, D., Lourenço, A., Silva, L., & Oliveira, L. (2010). "Reducing Forgeries in Handwritten Signature Verification Based on Texture Features." *Expert Systems with Applications*, 37(7), 5436–5443.
- [4] S. T. R. Kandula, "Cloud-Native Enterprise Systems In Healthcare: An Architectural Framework Using Aws Services," *International Journal Of Information Technology And Management Information Systems*, vol. 16, no. 2, pp. 1644–1661, Mar. 2025, doi: https://doi.org/10.34218/ijitmis_16_02_103
- [5] Vargas, J. F., & Ferrer, M. A. (2011). "Robust Off-line Signature Verification Using Writer-Independent Features." *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 33(10), 2106–2117.
- [6] Chen, S., Huo, Q., & Chen, L. (2019). "Offline Signature Verification Based on Convolutional Siamese Networks." *IEEE Access*, 7, 69675–69684.
- [7] Nguyen, H. H., & Zhang, J. (2018). "A Hybrid Feature Learning Approach for Offline Signature Forgery Detection." *International Journal of Computer Applications*, 181(33), 1–6.
- [8] Chen, Z., Lin, C. T., & Lee, C. S. (2017). "Signature Verification and Forgery Detection Using Image Processing and Machine Learning." *Journal of Computer Science*, 13(4), 105–113.
- [9] Eskander, G. S., Sabourin, R., & Granger, E. (2013). "Hybrid Writer-Independent–Writer-Dependent Offline Signature Verification System." *Pattern Recognition*, 46(5), 1308–1320.
- [10] Impedovo, D., & Pirlo, G. (2008). "Automatic Signature Verification: The State of the Art." *IEEE Transactions on Systems, Man, and Cybernetics*, 38(5), 609–635.
- [11] Hanmandlu, M., & Bhattacharya, J. (2007). "Off-Line Signature Verification Using Dynamic Features." *Pattern Recognition Letters*, 28(7), 862–869.
- [12] M. V. Sruthi, "Effective Adaptive Multilevel Modulation Technique Free Space Optical Communication," *Proceedings of Sixth International Conference on Computer and Communication Technologies*, pp. 223–229, Oct. 2025, doi: 10.1007/978-981-96-7477-0_19.
- [13] Malik, A., & Bansal, S. (2020). "Handcrafted and Deep Learning-Based Features for Offline Signature Forgery Detection." *International Journal of Biometrics*, 12(3), 233–249.
- [14] Paruchuri, Venubabu, *Securing Digital Banking: The Role of AI and Biometric Technologies in Cybersecurity and Data Privacy* (July 30, 2021). Available at SSRN: <https://ssrn.com/abstract=5515258> or <http://dx.doi.org/10.2139/ssrn.5515258>
- [15] Diaz, M., Ferrer, M. A., & Vargas, F. (2018). "Siamese Recurrent Networks for Offline Signature Verification." *IET Biometrics*, 7(4), 384–394.
- [16] Sankar Das, S. (2024). *Harnessing data lineage: making artificial intelligence smarter*

using data governance Frameworks.
International Journal of Research and Analytical
Reviews, 11(1).

<https://doi.org/10.56975/ijrar.v11i1.322571>

[17] Prodduturi, S.M.K. (2025). AI-Enhanced Mobile Application Development: Leveraging Machine Learning for Real-Time User Interaction. International Journal of Modern Engineering and Technology (IJMET), 15(2), pp.145–150.

[18] Yilmaz, E., & Ozturk, S. (2020). “Signature Forgery Detection Using Deep CNN and Image Hashing.” Procedia Computer Science, 176, 1454–1462.

[19] Kumar, R., & Sharma, A. (2019). “A Deep Learning Framework for Offline Signature Verification and Forgery Detection.” International Journal of Computer Engineering, 11(2), 55–62.

[20] Al-Maadeed, S., Khelifi, F., & Bouridane, A. (2014). “An Improved Texture-Based Approach for Offline Signature Verification.” IEEE Systems Journal, 8(3), 554–567.