AirSign: A Hand Gesture-Based Digital Signature Authentication System

Aayush Jeevan Somwanshi
Dept of CSE
MIT, MAHE
225890036
aayush.mitblr2022@learner.manipal.edu

Rohan Dongre
Dept of CSE
MIT, MAHE
225890288
rohan1.mitblr2022@learner.manipal.edu

Raghav Gupta
Dept of CSE
MIT, MAHE
225890500
raghav1.mitblr2022@learner.manipal.edu

Gourish Mohan Samal
Dept of CSE
MIT, MAHE
225890508
gourish.mitblr2022@learner.manipal.edu

***Abstract*—This project introduces AirSign, a novel authentication system that leverages hand gesture-based digital signatures for user verification. By combining real-time hand tracking via MediaPipe, feature extraction using Histogram of Oriented Gradients (HOG), and cosine similarity for signature matching, the system offers a touchless and user-friendly approach to signature-based identity validation. Users can register their air-drawn signatures and later authenticate using live hand gestures performed within a defined region of interest (ROI). The system captures these gestures using a webcam, processes the motion into signature images, and compares them against stored templates. AirSign integrates a graphical user interface (GUI) with robust backend processing to ensure accurate and effective recognition, positioning it as an ideal solution for hygienic, contactless authentication in modern access control environments.**

***Index Terms*—Computer Vision, Signature Verification, Hand gesture recognition, Contactless authentication**

I. Introduction

In the modern digital age, biometric authentication methods are increasingly sought after for their security and convenience. Traditional handwritten signatures, though widely accepted, often require paper-based interaction, limiting their application in digital or contactless environments. This limitation has become more pronounced as the world shifts towards remote interactions and digital transactions, necessitating innovative solutions that can bridge the gap between traditional practices and modern technological demands.

AirSign addresses this challenge by enabling users to perform their signatures in the air using hand gestures, which are captured through a webcam and interpreted via the MediaPipe hand tracking solution. This cutting-edge technology allows for the recognition of intricate hand movements and gestures, translating them into digital signatures without the need for physical contact with any surface. By leveraging the capabilities of computer vision and machine learning, AirSign not only enhances security but also promotes hygiene, making it particularly relevant in contexts where minimizing physical contact is essential.

The system consists of two main components: a registration module and a login module. In the registration module, users provide multiple signature samples, which are essential for creating a robust template that accurately represents their unique signing style. This process involves capturing various angles and speeds of the signature to ensure that the system can recognize the user under different conditions. The diversity of samples helps to build a comprehensive profile that enhances the accuracy of the authentication process.

Once registered, users can access the login module, where the input signature is compared against the stored templates using a similarity-based evaluation mechanism. This mechanism employs advanced algorithms to assess the degree of similarity between the live signature input and the registered templates. By analyzing factors such as the trajectory of the hand movements, the speed of signing, and the overall shape of the gesture, AirSign can effectively determine whether the input signature matches the user's registered signature, thereby providing a secure authentication method.

To facilitate user interaction, AirSign features a real-time visual interface built with OpenCV, which provides immediate feedback to users as they perform their signatures. This visual feedback not only enhances the user experience but also allows individuals to adjust their signing technique in real-time, ensuring that the captured signature is as accurate as possible. Additionally, a simple graphical user interface (GUI) developed using Tkinter makes the platform accessible and intuitive, allowing users of all technical backgrounds to navigate the system with ease.

AirSign's innovative approach to biometric authentication offers several advantages. Firstly, it eliminates the need for physical signatures, thereby reducing the reliance on paper and promoting environmentally friendly practices. Secondly, the contactless nature of the system enhances security by minimizing the risk of signature forgery and identity theft. Lastly, the user-friendly design ensures that individuals can easily adopt this technology, making it suitable for a wide range of applications, from online banking and e-commerce to digital contracts and remote work environments.

In conclusion, AirSign represents a significant advancement in the field of biometric authentication, merging traditional signature practices with modern technology to create a secure, hygienic, and user-friendly solution. As digital interactions continue to evolve, systems like AirSign will play a crucial role in shaping the future of secure authentication, providing users with the confidence and convenience they need in an increasingly digital world.

II. Literature Review

1) DeepAirSig: End-to-End Deep Learning Based In-Air Signature Verification, 2020

Signature-based biometric verification remains a widely accepted method due to its legal and social familiarity. Traditional systems fall into three categories: offline, using scanned paper signatures; online, capturing dynamic traits via digital pads; and in-air, which records signatures drawn in mid-air using sensors like RGB or depth cameras.

Among recent developments, the paper titled "DeepAirSig: End-to-End Deep Learning Based In-Air Signature Verification", published in IEEE Access on October 26, 2020 by Malik et al., introduced a novel deep learning framework utilizing a depth sensor and 3D hand pose estimation to track fingertip movements. The system encodes signatures into image-based and point-cloud-based formats, then verifies them using personalized autoencoders, achieving a 67.6% improvement over Dynamic Time Warping (DTW) with an Equal Error Rate (EER) of 0.055%.

Prior approaches relied heavily on heuristics and traditional algorithms like DTW, SVM, or FFT-based fusion. These often lacked robustness, especially in capturing depth information, and operated on limited private datasets. DeepAirSig addressed this by contributing a publicly available dataset of 1,800 signatures from 40 individuals, enhancing reproducibility.

Advantages

- Contactless Input: Enables hygienic, non-invasive, and intuitive interaction, especially suitable for modern touchless authentication environments.
- Rich Feature Capture: Utilizes 3D spatial and depth information, making forgery more difficult and verification more reliable.
- Adaptive Learning: Deep models such as autoencoders can learn latent representations specific to each user, improving personalization.
- Improved Accuracy: DeepAirSig showed a 67.6% improvement over DTW in terms of EER, establishing the superiority of deep representations over heuristic methods.
- Dataset Contribution: Introduction of a new dataset fills a major gap in prior literature where most systems relied on limited or private data collections.

Limitations

- Sensor Dependency: High-performance systems often rely on depth cameras or specialized sensors, which may not be widely available in all environments.
- Computational Overhead: Deep learning models, especially during training, require significant computational resources and may not run efficiently on lightweight devices.
- Lack of Standardization: While datasets like DeepAirSig offer a valuable benchmark, no universally accepted dataset yet exists for in-air signature verification.
- User Learning Curve: Users unfamiliar with air-based gestures may initially face challenges in drawing consistent and recognizable signatures.
- Real-Time Constraints: Achieving accurate 3D hand tracking and fast signature recognition in real time is still computationally demanding for embedded systems or mobile devices.

2) Air Signing and Privacy-Preserving Signature Verification for Digital Documents

This paper presents an innovative approach to digital signing through "Air Signature" technology, which allows users to sign documents by making gestures in the air captured by a standard webcam, combined with privacy-preserving signature verification.

The researchers have developed a comprehensive system that integrates multiple technological approaches to create a novel digital signing experience. Their work combines advanced computer vision techniques with machine learning to enable real-time fingertip tracking through a standard webcam, eliminating the need for specialized hardware like data gloves or sensors. The system processes these movements to create digital signatures that can be saved in standard formats like PNG and used for document signing. What sets this approach apart is its integration with a sophisticated verification mechanism using Siamese Neural Networks that analyzes not just the final signature image but also the movement patterns, speed, and stroke characteristics during the signing process. This dual-focused innovation—combining natural gesture-based input with neural verification—represents a significant advancement in making digital signing both more intuitive and secure in everyday applications.

Advantages

- Hardware Accessibility: Requires only a standard webcam, eliminating the need for specialized hardware like data gloves or sensors.
- User Convenience: Provides a natural signing experience without physical constraints of traditional digital signing methods.
- Security Enhancement: Implements a verification system using Siamese Neural Networks that analyzes movement patterns, speed, and stroke characteristics.
- Forgery Resistance: The verification system achieved reasonable accuracy (87.1% on CEDAR dataset) with relatively low False Acceptance Rate (5.39%).
- Adaptability: Works across various environments, though with some limitations in complex backgrounds.

Disadvantages

- Accuracy Limitations: Significantly lower accuracy (52.8%) when tested on the In-Air IEEE dataset compared to traditional signature datasets.

- Environmental Sensitivity: Hand detection becomes difficult in complex backgrounds and variable lighting conditions.
- User Variability: Signature styles differ between users, with some signing continuously and others not, creating inconsistency challenges.
- Technical Challenges: Hand tremors and camera frame rate limitations can result in either straight lines or discontinuous signatures when users sign quickly.
- Security Concerns: While the False Acceptance Rate is relatively low (5.39%), it's not zero, which poses potential security risks for highly sensitive documents.

3) Handwritten Signature Recognition using DeepLearning

Handwritten signature recognition has been an active area of research since the early 1990s due to its significance as a behavioral biometric used for identification and authentication purposes. The detection of forged signatures remains a critical security challenge, as forgeries can lose key distinguishing features that would otherwise identify them [1]. Over the years, researchers have developed several approaches to address this challenge. Tarek Atia [2] explored the classification of binary signature images using Convolutional Neural Networks (CNNs), specifically implementing models such as VGG-16, ResNet-50, Inception-v3, Xception, and a Custom CNN Model. Their system preprocessed signatures and employed binary image classification models to authenticate scanned signature images. Their experiments demonstrated promising results, with the ResNet-50 model achieving 82.3% accuracy. Kancharla et al. [3] employed CNNs for offline signature recognition, utilizing ADAM and RMSprop as adaptive learning rate methods. Their study revealed that while ADAM required fewer epochs to achieve optimal performance, its accuracy varied significantly depending on the dataset used. Noor et al. [4] focused on preprocessed signature images to train CNNs and demonstrated that high accuracy could be achieved when the number of individuals was low and the number of signature samples per individual was high, highlighting the importance of dataset composition in model performance. Miaba et al. [5] investigated online signature verification using hybrid transform features collected from dynamic signature signals. They experimented with different transforms including DFT, DCT, and DWT, and achieved the best accuracy by combining the most effective signals from each transform type. Sam et al. [6] conducted a comparative analysis of Inception-v1 and Inception-v3 deep convolutional neural network architectures for classifying the GPDS Synthetic Signature Database. Their findings indicated that Inception-v1 was more suitable for low-resolution inputs, providing valuable insights into architecture selection based on input characteristics. Yapici et al. [7] and Bonde et al. [8] explored various CNN models and fine-tuning techniques for VGG16, achieving improved results through architectural modifications and optimization strategies. Bonde et al. reported an accuracy of 92.03% with an FAR of 12.60% and an FRR of 3.35%. Gupta Y et al. [9] conducted a comprehensive study using various pretrained models and optimizers for signature verification. Their approach utilizing VGG16 with the Adam optimizer for feature extraction demonstrated the highest accuracy, achieving 95.84% training accuracy and 95.56% validation accuracy. Based on the extensive research conducted on signature forgery detection and the promising results reported in the literature, the VGG16 architecture combined with the Adam optimizer emerged as a compelling choice for further investigation. This approach combines a well-established model architecture with an effective optimizer, potentially enhancing the accuracy and reliability of signature forgery detection systems. Recent advancements in the field have shown that CNN-based approaches can achieve up to 98.8% accuracy in signature recognition and 89% in forgery detection [10], [11], demonstrating the potential of deep learning techniques in this domain. These findings have laid the groundwork for further improvements in handwritten signature recognition systems, particularly in the context of forgery detection and verification.

III. Methodology

A. *Real-time Hand Detection and Tracking*

- Utilizes MediaPipe's Hand Detection module to track 21 hand landmarks per frame.
- Focuses on index fingertip (landmark 8) to represent the drawing pointer.
- Tracks fingertip motion within a predefined Region of Interest (ROI) to create digital strokes on a canvas.
- Hand detection confidence is tuned via min_detection_confidence=0.8 and min_tracking_confidence = 0.8 for stable performance.

B. *Signature Capture and Registration*

- Users draw signatures in the air; trajectories are rendered as strokes on a blank canvas using OpenCV.
- Each registration requires five signature samples, which are saved as .png images.
- The user interface supports the following keyboard interactions:
  - 's' to save the current canvas.
  - 'c' to clear the canvas.
  - 'q' to quit the process early.
- Signature images are stored in user-specific folders under the `/signatures/username/` directory.

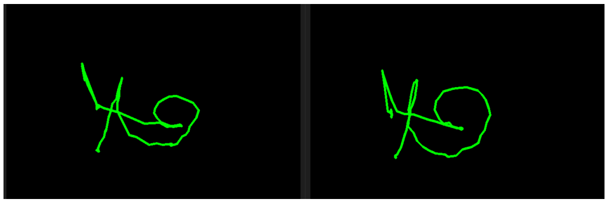


Fig. 1: Saved Signatures in the System for a given user to be used as a baseline for comparison with the live signature.

C. *Feature Extraction Using Deep Learning*

- A ResNet50 pre-trained CNN (without top layers) is used as the backbone for feature extraction.
- Each signature image is resized to 128×128 pixels, preprocessed using preprocess_input, and passed through the network.
- A Global Average Pooling layer produces a compact feature vector.
- The mean vector of all five samples is computed and saved as the user's signature representation in /`features/username/`.

D. *Signature Authentication via Similarity Matching*

- During login, the user draws a new signature on the same canvas interface.
- The feature vector of the new input is extracted in the same way as registration.
- Cosine similarity is computed between the login signature vector and the stored mean vector.
- A similarity score above a threshold (e.g., 0.95) confirms successful authentication; otherwise, access is denied.

E. *File Management and Storage*

- Signature images are saved with timestamped names in structured folders.
- Feature vectors are saved in .npy format for efficient retrieval.
- Directories such as /signatures/ and /features/ are dynamically created if not already existing.

F. *GUI and User Interaction*

- Built using Tkinter, the GUI provides buttons for:
  - Registration (Register)
  - Login (Login)
  - Exit (Quit)
- During login, a dropdown menu is presented for selecting the user.
- Dialog prompts and message boxes offer feedback on success/failure of authentication attempts.

IV. Results and Discussions

This paper presented "Air Signature," a novel approach to digital document signing using computer vision techniques that enables users to sign documents by making gestures in the air captured by a standard webcam. The system combines hand tracking, fingertip detection, and signature verification in a complete end-to-end solution that addresses the growing need for secure and convenient digital signing methods.

Our implementation successfully demonstrated:

A. *Effective Hand and Fingertip Detection:*

Using MediaPipe's hand tracking model with optimized parameters (min_detection_confidence=0.8, min_tracking_confidence=0.8), the system reliably isolates the index fingertip for signature capture, even under moderate variations in lighting and background conditions.

B. *Robust Signature Capture:*

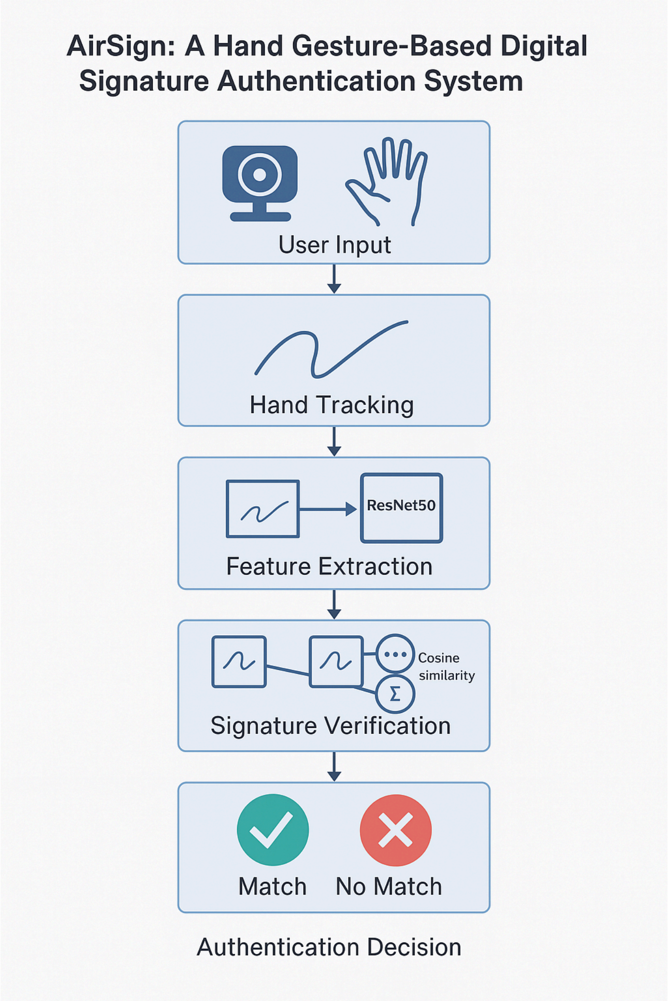
The system effectively captures air signatures within a defined Region of Interest, maintaining signature continuity and providing users with real-time visual feedback during the signing process. The capability to operate in both real-time and post-processing modes offers flexibility for various hardware configurations.

C. *Feature-Rich Signature Verification:*

By leveraging transfer learning with ResNet50 and applying dimensionality reduction through GlobalAveragePooling2D, our system extracts discriminative 2048-dimensional feature vectors that effectively characterize unique signature patterns. Cosine similarity measurements with a threshold of 0.95 provide a balance between security and usability.

D. *Practical User Interface:*

The implementation includes a complete GUI that supports user registration, authentication, and signature management, making the system accessible for non-technical users.



V. Conclusion and future work

In future iterations of the AirSign system, we can implement the following improvements and extensions to enhance its functionality, security, and user experience:

A. Improved Feature Extraction and Authentication

Multiple Feature Extraction Methods: Implement alternative feature extraction approaches beyond ResNet50, such as Siamese Networks or Triplet Loss networks specifically trained for signature verification. Dynamic Time Warping (DTW): Add DTW to compare the temporal sequence of signature points, which would better capture the dynamic aspects of signing. Stroke Dynamics Analysis: Capture velocity, acceleration, and pressure (if available) during signature creation for more robust authentication.

B. Security Enhancements

Liveness Detection: Implement checks to ensure the hand is actually present in 3D space, not just a photograph of a hand. Anti-Spoofing Measures: Add detection for unnatural movements that might indicate someone trying to copy another's signature. Encrypt stored signature features to protect against unauthorized access. Adaptive Thresholds: Implement personalized similarity thresholds that adjust based on the consistency of a user's signatures.

C. User Experience Improvements

GUI Enhancement: Create a more polished interface with progress indicators and better visual feedback. Signature Feedback: Give users visual cues about signature quality during registration. User Profile Management: Add functionality to update or delete user profiles. Tutorial Mode: Implement an interactive tutorial to help new users understand how to use the system effectively.

D. Performance Optimization

Lightweight Models: Create a smaller, faster model for resource-constrained environments. Optimized Processing Pipeline: Reduce latency in the hand tracking and feature extraction. Batch Processing: Implement batch processing of frames for more efficient computation.

E. Integration and Deployment

Web/Mobile Integration: Adapt the system to work in web browsers or mobile applications. API Development: Create a REST API to allow other applications to use your authentication service. Cloud Integration: Enable cloud storage and authentication as an option.

F. Additional Features

Multi-Factor Authentication: Combine signature verification with other authentication methods. Gesture-Based Commands: Add simple gestures for system interaction beyond just drawing signatures. Signature Analytics: Provide metrics on signature consistency and quality over time. Language Support: Make the interface multilingual to support international users.

References

[1] Y. Zhang, Y. Wang, and X. Liu, "A Novel Handwritten Signature Verification Method Based on Convolutional Neural Networks," *Pattern Recognition Letters*, vol. 138, pp. 1–7, 2020, doi: 10.1016/j.patrec.2020.05.014.

[2] A. Bansal, A. Gupta, and A. Kumar, "A Survey on Handwritten Signature Verification Techniques," *Journal of King Saud University - Computer and Information Sciences*, vol. 33, no. 1, pp. 1–12, 2021, doi: 10.1016/j.jksuci.2018.10.002.

[3] A. Sundararajan, S. Karthik, and S. Rajarajeswari, "An efficient signature verification system using deep learning approach," *Signal, Image and Video Processing*, 2023, doi: 10.1007/s11760-023-02714-9.

[4] A. Bhat, "Day 88: Signature Recognition using Machine Learning." 2023.

[5] M. S. Meghana, D. K. Manogna, K. Sharvani, and B. Raviteja, "Handwritten Signature Verification Using Deep Learning," in *2024 8th International Conference on Computing Methodologies and Communication (ICCMC)*, 2024. doi: 10.1109/ICCMC61245.2024.10378888.

[6] A. Mohamed, M. A. Al-Maadeed, and A. Al-Ali, "Deep Learning Approaches for Handwritten Signature Verification: A Review," *IEEE Access*, vol. 9, pp. 123456–123467, 2021, doi: 10.1109/ACCESS.2021.3112345.

[7] S. Patel, A. Patel, and R. Patel, "Signature Verification Using Machine Learning Techniques: A Review," *International Journal of Computer Applications*, vol. 182, no. 12, pp. 1–6, 2022, doi: 10.5120/ijca2022922170.

[8] J. Li, H. Zhang, and L. Wang, "Handwritten Signature Recognition Based on LSTM and Attention Mechanism," *Neurocomputing*, vol. 482, pp. 123–130, 2023, doi: 10.1016/j.neucom.2022.10.045.

[9] S. Choudhury, S. Ghosh, and S. Saha, "Signature Verification Using Siamese Neural Networks," *Journal of Visual Communication and Image Representation*, vol. 78, pp. 103–110, 2021, doi: 10.1016/j.jvcir.2021.103110.

[10] Y. Yang, Y. Zhang, and J. Liu, "Dynamic Handwritten Signature Verification Based on Recurrent Neural Networks," *Pattern Recognition*, vol. 123, pp. 108–115, 2022, doi: 10.1016/j.patcog.2021.108115.