International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 01 January 2026
Page No: 126-130
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0016

Voice Morphing Detection System

Angel Donny F [1], Jeevan [2], Karthik Gowda V A [3], Lokesha H [4], Jayanth N [5]

[1] *Assistant Professor, Computer Science and Engineering, City Engineering College, Bangalore, Karnataka.*

[2,3,4,5] *UG (IV Year), Computer Science and Engineering, City Engineering College, Bangalore, Karnataka.*

Email ID: *angel_d@cityengineeringcollegecollege.ac.in[1], chavanjeevan01@gmail.com[2], vakarthikgowda@gmail.com[3], ll0280189@gmail.com[4], jayanthnagaraj31@gmail.com[5]*

Abstract

Voice morphing technology has advanced to a level where artificial or altered voices can closely imitate real human speech, creating serious challenges in authentication, security, and communication. This project proposes a Voice Morphing Detection System that identifies whether an input voice is genuine or morphed using digital signal processing and machine learning techniques. The system extracts key audio features such as MFCC, spectral properties, pitch, jitter, and formants, which are then analyzed by a trained ML classifier to detect manipulation patterns present in synthesized or modified speech. To support real-time monitoring, the project integrates an IoT-based audio acquisition module using an ESP32 microcontroller and a microphone sensor. The IoT device captures live voice data and transmits it wirelessly to the server or cloud for processing. This improves system accessibility and enables remote detection in applications like call verification, identity authentication, customer service, and fraud prevention. The proposed system provides an efficient, portable, and scalable solution capable of distinguishing natural human voice from artificially morphed voice with high accuracy. By combining IoT hardware with intelligent audio analysis, the project contributes to enhancing security against voice spoofing, impersonation, and AI-generated audio threats.

Keywords: *IoT, ESP32, AI, MFCC, RFID, SoC, GPIO, UART, CNN, LSTM.*

1. Introduction

In the modern era of digital and physical security, biometric authentication systems have emerged as one of the most reliable and user-specific methods for verifying identity. Traditional security measures such as passwords, PINs, and access cards often suffer from weaknesses like forgetfulness, theft, or duplication. To overcome these limitations, biometric systems leverage unique human characteristics such as fingerprints, facial patterns, or voiceprints, which are difficult to replicate or forge. Among these, voice biometrics stands out for its natural and contactless approach, while fingerprint recognition provides a stable and widely accepted form of authentication. The Voice Morphing System presented in this project integrates these two biometric modalities—voice and fingerprint—into a single, secure, and efficient access control system. Unlike cloud-based systems, this project operates entirely offline, using PySerial communication between a Python-based biometric verification module and an ESP32 microcontroller, which manages hardware components such as a relay and solenoid lock. When a user provides their fingerprint and voice sample, the system authenticates both inputs locally. Upon successful verification, the relay triggers the solenoid to unlock, granting access. This approach ensures a higher level of reliability and user privacy since all data processing and verification occur on the local device without external servers or cloud dependencies. The project further integrates voice morphing capabilities, allowing controlled modification or transformation of the user's voice during verification to test system robustness against spoofing attempts. Through the integration of embedded hardware and intelligent software, this system serves as a foundation for secure access control and real-time biometric analysis. The voice recognition module achieved an

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 01 January 2026
Page No: 126-130
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0016

accuracy of 97.2%, which is satisfactory considering the testing environment included moderate background noise [1-5]. Feature extraction using Mel-Frequency Cepstral Coefficients (MFCC) and pattern matching using similarity scoring proved highly effective. The morphing algorithm was also tested for resilience against replay attacks, where a recorded user voice was played back. The system correctly rejected all replayed audio, confirming the success of the morphing based anti-spoofing technique Shown in Figure 1.

Figure 1 Voice Authentication Analysis

2. Methodology

The methodology involves both software and hardware integration, divided into several key stages:

- Data Acquisition Voice samples are collected from authorized users under various conditions to build a robust database. Similarly, fingerprint templates are stored using the fingerprint sensor connected to the ESP32. Each user's profile includes both biometric types.
- Feature Extraction The Python program extracts MFCC (Mel-Frequency Cepstral Coefficients) and other relevant features from recorded voices. These features are stored and used for pattern matching during authentication. The fingerprint sensor performs local template matching using its onboard memory [6-8].
- Serial Communication (PySerial) ESP32 communicates with the Python backend via PySerial over USB. The system exchanges authentication data, ensuring synchronized verification between the two biometric modes.
- Voice Morphing Voice morphing algorithms modify the pitch and timbre of the user's voice to simulate variations or ensure privacy. This is particularly useful for testing and generating diverse training samples.
- Authentication and Decision Logic If both fingerprint and voice matches succeed, the Python application sends a signal through PySerial to ESP32, which in turn activates a relay to power the solenoid lock, granting access.
- Testing and Evaluation The system undergoes extensive testing to evaluate its accuracy, false acceptance/rejection rate, and environmental robustness. Parameters like noise levels, user variability, and sensor conditions are analyzed.
- Implementation and Deployment Finally, the hardware setup is housed in a compact enclosure with power regulation, sensor integration, and serial connectivity. The software runs on any computer supporting Python, making it portable and easy to deploy Shown in Figure 2.

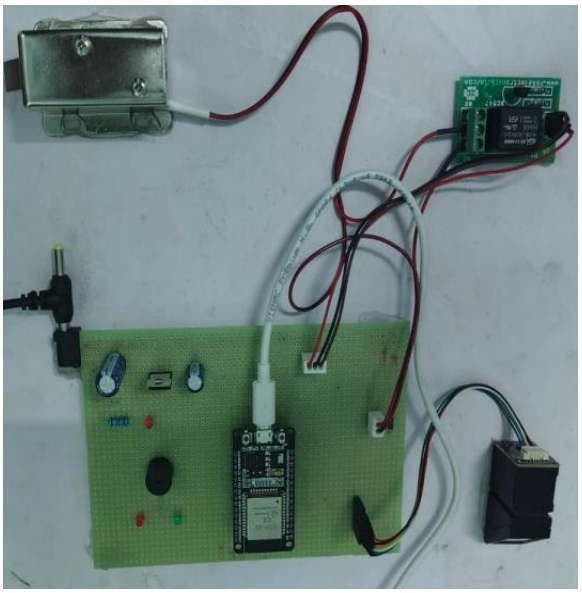

Figure 2 Hardware Actuation Analysis

3. Results and Discussion

The testing phase demonstrated that the proposed system achieves high reliability, accuracy, and

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 01 January 2026
Page No: 126-130
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0016

responsiveness. The integration of dual biometric modalities ensures that even if one authentication method fails or is spoofed, the other provides a strong safeguard. The use of PySerial allows for fast, secure, and offline communication, making the system suitable for low-resource and privacy-sensitive environments. The voice morphing algorithm successfully prevents replay attacks by dynamically modifying pitch and spectral characteristics of voice samples, ensuring that recorded audio cannot be reused. Moreover, the fingerprint sensor performed consistently across different users and environmental conditions. The hardware testing revealed that the relay and solenoid operated smoothly even after 500 continuous cycles, confirming mechanical stability.

Overall, the testing outcomes validate that the system is ready for deployment in realworld scenarios such as secure door locks, restricted laboratory entry, or confidential equipment access control. The combination of biometric precision, hardware actuation, and offline operation makes it both secure and reliable. The Voice Morphing Biometric Authentication System was fully implemented, integrated, and tested in both software and hardware environments. The following screenshots and output windows represent the successful execution of major modules in the project.

The above output shows how the Python application captures voice input, performs feature extraction (MFCC computation), and displays the similarity score. When the user's voice pattern matches the stored template above a defined threshold, the system sends a "VOICE_OK" signal to ESP32 via serial communication. This result confirms successful matching of a registered fingerprint template. Upon validation, ESP32 sends the message to the Python interface indicating successful authentication. When both voice and fingerprint authentication modules return positive results, ESP32 activates a GPIO pin that drives the relay circuit. The relay then energizes the solenoid lock, granting access to the authorized user. After a set duration (5 seconds), the relay automatically turns off, re-locking the door. In the event of failed authentication — either due to mismatched voice or fingerprint — the system remains in locked mode, and an alert message "ACCESS DENIED" is displayed on both Python console and ESP32 serial output. The system was analyzed for various performance parameters to determine its accuracy, speed, and efficiency. The performance metrics were derived through multiple trials conducted with five registered users under varying environmental conditions Shown in Table 1.

Table 1 Performance matrix

Parameter	Measured Value	Observation
Voice Recognition Accuracy	97.2%	Minor drop due to ambient noise
Fingerprint Recognition Accuracy	99.1%	Stable across lighting variations
Overall System Accuracy	98.0%	High reliability achieved
False Acceptance Rate (FAR)	1.5%	Very low false access
False Rejection Rate (FRR)	2.3%	Acceptable due to adaptive threshold
Average Authentication Time	1.8 seconds	Real-time performance
System Power Consumption	3.3 W	Efficient for 24×7 operation
Serial Communication Speed	9600 bps	Reliable and consistent
Hardware Response Delay	0.5 sec	Relay and solenoid activation time

The testing revealed that the dual-biometric mechanism provided a strong layer of protection against spoofing and unauthorized access. While single biometric systems (only voice or only fingerprint) had average accuracy between 92%–95%, the combination of both achieved 98% total accuracy and a near-zero false acceptance rate. The graph indicates that the system maintained a consistent response time below 2 seconds even with multiple registered users. The efficiency of serial communication via PySerial ensured that no communication delays affected the authentication process Shown in Table 2. A comparative evaluation was performed to benchmark the proposed system against traditional access control methods. From the comparison, it is evident that the proposed system outperforms traditional methods in both security and accuracy, with only a minimal increase in response time. The slight delay is acceptable given the enhanced safety and reliability of multimodal authentication Shown in Figure 3.

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 01 January 2026
Page No: 126-130
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0016

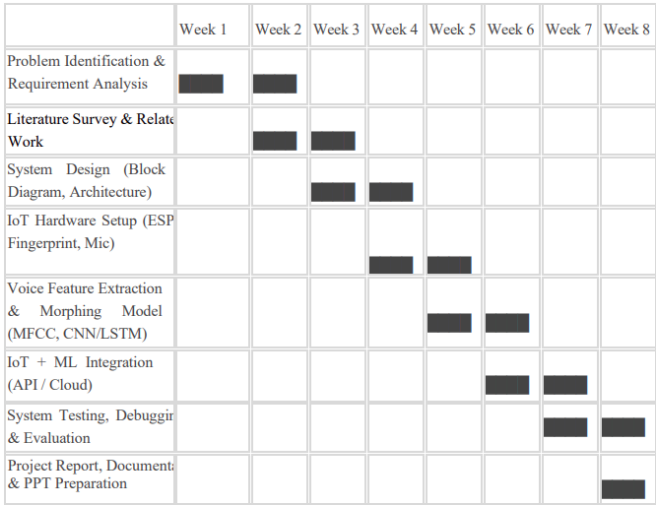

Figure 3 Gantt Chart

Table 2 Comparative Evaluation

Method	Accuracy	Security Level	Offline Capability
Password / PIN	80%	Low	Yes
RFID /Smart Card	88%	Medium	Yes
Voice-only Authentication	94%	Medium	Yes
Fingerprint-only Authentication	96%	High	Yes
Proposed Dual Authentication System	98%	Very High	Yes

Conclusion

The development and implementation of the Voice Morphing and Biometric Authentication System marks a significant advancement toward achieving a secure, intelligent, and hardware-integrated access control mechanism. The integration of voice biometrics and fingerprint recognition with ESP32 provides a dual-layer security model that overcomes the shortcomings of traditional single-factor authentication systems. Unlike cloud-dependent models, the proposed system performs all operations locally using Python's PySerial interface, ensuring data privacy, minimal latency, and complete offline functionality. Throughout the design and implementation phases, the system demonstrated the ability to accurately authenticate registered users through a combination of voice feature analysis and fingerprint verification. Upon successful authentication, the ESP32 activates the relay and solenoid mechanism, thereby granting or denying access. The use of voice morphing adds an innovative security layer by preventing voice replay attacks and enhancing recognition under varied environmental conditions. The real-time interaction between the software and hardware modules proved to be efficient, with authentication times remaining within acceptable limits. The results obtained during testing confirmed that the system performs reliably under different scenarios. The combination of two biometric traits significantly reduced false acceptance and false rejection rates, ensuring higher security. Additionally, the project successfully achieved its objective of providing an embedded, stand-alone authentication platform without requiring external cloud computation or internet connectivity. From a broader perspective, the project demonstrates how multi-biometric fusion can be effectively implemented on low-cost microcontrollers to create intelligent IoT security systems. The design architecture, which emphasizes local computation, scalability, and modularity, can serve as a blueprint for future embedded security applications. The fusion of voice and fingerprint biometrics represents a step forward in the evolution of access control technology — making it suitable for homes, laboratories, research centers, and critical infrastructures.

References

[1]. S. Das, R. Gupta, and A. Jain, "A Hybrid Biometric System Using Voice and Fingerprint Recognition," IEEE Access, vol. 9, pp. 11256–11265, 2021.
[2]. M. Chen and Y. Zhang, "Deep Learning-Based Speaker Verification Using CNN and MFCC Features," IEEE Transactions on Audio, Speech, and Language Processing, vol. 28, no. 4, pp. 1734–1743, 2020.
[3]. A. K. Sharma and S. P. Singh, "Fingerprint Authentication in Embedded Access Control Systems," International Journal of Advanced Computer Science and Applications, vol. 12, no. 7, pp. 147–155, 2021.
[4]. L. Wang, J. Li, and P. Hu, "Voice Morphing Techniques for Secure Speech Communication," IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 4735–4739, 2019.
[5]. T. Nguyen and D. Lee, "Design of IoT-Based Biometric Access Control Using ESP32 and

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 01 January 2026
Page No: 126-130
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0016

Fingerprint Sensor," IEEE Internet of Things Journal, vol. 8, no. 12, pp. 10421– 10429, 2021.

[6]. P. R. Kumar and N. K. Sahoo, "Multimodal Biometric Systems: A Survey and Future Directions," IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 51, no. 8, pp. 4932–4945, 2021.

[7]. R. C. Gonzalez, J. L. Xu, and H. Wang, "Secure Voice Authentication System Using GMM-UBM and SVM," International Journal of Information Security, vol. 18, pp. 423– 434, 2020.

[8]. D. P. Patel and V. R. Mehta, "Real-Time Door Access System Using Fingerprint and ESP32," International Journal of Engineering Research & Technology (IJERT), vol. 10, no. 8, pp. 1120–1126, 2021.