iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

DESIGN AND IMPLEMENTATION OF A VOICEPRINT RECOGNITION SYSTEM FOR HYBRID SECURITY AND AUTHENTICATION IN A UNIVERSITY ORGANIZATIONAL INFRASTRUCTURE

Adedeji A. Abdulhameed[1], John Bosco Ssemakula[2], Olalere O. Abbas[3], Adedeji A. AbdulAzeez[4], Adedeji A. Ahmed[5]
[1, 4, 5] A.I & Robotics Division, Foresight Institute of Research and Translation, Nigeria.
[2]Kyambogo University Uganda.
[3]Powerflo Nig. Ltd.
[4]Department of Electronics and Telecommunication Engineering, University of Rwanda.
[5]Department of Pharmacology & Toxicology, University of Rwanda.

ABSTRACT
Voiceprint recognition, a unique biometric modality, offers a secure and efficient alternative to conventional password-based authentication systems. This paper presents the design and implementation of a hybrid biometric authentication system that integrates voiceprint and fingerprint recognition to enhance security in university organizational infrastructures. The system leverages the Raspbian operating system and SOPARE software to capture, process, and authenticate voiceprints, while a fingerprint module provides an additional layer of verification. By combining these two biometric modalities, the system significantly reduces the risk of unauthorized access and impersonation attacks. The proposed solution Overcomes key voice recognition challenges, such as key challenges in voice recognition, such as background noise and spoofing, through a robust algorithmic design and multi-modal verification. Furthermore, the potential applications of the system go beyond university security and offer potential use cases in education, agriculture and healthcare. This work, demonstrating the feasibility of a cost-effective, scalable, and user-friendly biometric authentication system, paves the way for future research in multi-modal biometric technologies.

Keywords:
Voiceprint Recognition, Biometric Authentication, Security Architecture, Raspbian OS, SOPARE Software

INTRODUCTION

As digital platforms become increasingly integral to both government and private services, the need for secure and efficient authentication systems has grown exponentially. Traditional password-based systems, while widely used, are vulnerable to breaches, phishing attacks, and user inconvenience [1]. In response, biometric authentication methods, such as voice and fingerprint recognition, have emerged as more reliable alternatives. These methods leverage unique physiological and behavioral traits, making them inherently more secure and difficult to replicate [2].

Voice recognition technology, in particular, has gained prominence due to its non-intrusive nature and ease of integration into existing systems. By analyzing unique vocal patterns, voice recognition systems can accurately identify and authenticate individuals, offering applications in access control, financial transactions, and personalized user experiences [3]. However, voice recognition systems face challenges such as background noise, spoofing attacks, and variability in speech patterns, which can compromise their reliability [4]. Recent advancements in deep learning and artificial intelligence (AI) have significantly improved the robustness of voice recognition systems, enabling them to perform well even in noisy environments [5,27,28]. To address these limitations, multi-modal biometric systems that combine voice recognition with other biometric modalities, such as fingerprint or facial recognition, have been proposed. These systems enhance security by cross-verifying multiple traits, thereby reducing the likelihood of unauthorized access [6].

This paper presents the design and implementation of a hybrid biometric authentication system that integrates voiceprint and fingerprint recognition for enhanced security in university organizational infrastructures. The proposed system leverages the Raspbian OS and SOPARE software to capture and process voiceprints, while a fingerprint module provides an additional layer of verification. By combining these two biometric modalities,

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

the system addresses key challenges in voice recognition, such as background noise and spoofing, and offers a robust solution for secure access control.

The contributions of this work are threefold:

1. Novel Hybrid Approach: The integration of voice and fingerprint recognition provides a multi-modal authentication system that enhances security and reduces vulnerabilities [7]. Recent studies have shown that hybrid systems significantly improve accuracy and resilience to spoofing attacks [8].
2. Cost-Effective Implementation: The use of Raspberry Pi and open-source software (SOPARE) demonstrates the feasibility of a low-cost, scalable biometric system [9]. This approach aligns with the growing trend of leveraging affordable hardware for advanced biometric applications [10,28].
3. Broad Applicability: While the system is designed for university security, its applications extend to other sectors, including education, agriculture, and healthcare, where secure and efficient authentication is critical [11]. For example, voice recognition has been successfully deployed in telemedicine and smart farming, demonstrating its versatility [12].

The remainder of this paper is organized as follows: Section II provides a comprehensive literature review of voice recognition technologies and their applications. Section III details the system design, including the enrollment and verification processes. Section IV discusses the implementation and testing of the system, while Section V explores its potential applications in various industries. Finally, Section VI concludes the paper and outlines future research directions.

LITERATURE REVIEW

As globalization, networking, and the digital era advance, the demand for high-reliability identity verification grows. Biometric methods have emerged as an efficient means of authenticating users by leveraging unique physiological or behavioral traits. Among existing biometric methods, voice biometrics stand out as an affordable and accurate authentication technology that has been successfully and widely employed. Voiceprint, as a basic human physiological characteristic, is difficult to counterfeit or replicate and plays a unique role in biometric security [13].

As a non-contact identification technology, voice recognition has gained acceptance for its user-friendliness and accuracy. Voice authentication involves accepting or rejecting the identity claim of a speaker based on the individual characteristics encoded in their speech waveform. Over the past two decades, this approach has been increasingly used as a convenient alternative to traditional password systems [14].

Voiceprint recognition is distinct from speech recognition. Voice recognition focuses on identifying speakers based on unique vocal traits, while speech recognition involves interpreting the content of spoken words. Speech recognition systems convert speech into text by capturing and analyzing complex acoustic signals. This process requires several steps, including:

1. Extracting discriminating speech features.
2. Applying sub-bound models and lexicons.
3. Determining phonemes spoken.
4. Applying grammatical rules to constrain word recognition.
5. Mapping phonemes to words and sentences [15].
6.

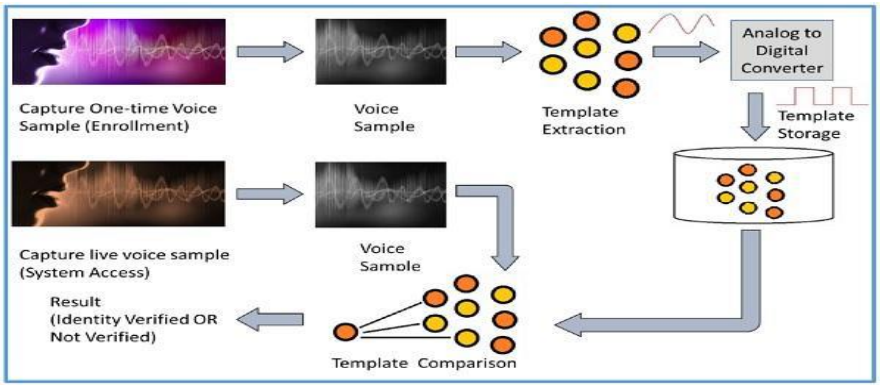

Fig 1. How speech recognition works

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

Voice recognition, on the other hand, emphasizes unique vocal characteristics and is independent of the spoken content. This technology enables applications like phone banking, database access, and home automation. Zhang and Wang (2020) highlighted that integrating speech and voice recognition systems has created hybrid models capable of both speaker identification and speech interpretation, enhancing their usability [16].

In early implementations, Gadalla (2006) demonstrated the use of voice recognition in the Massey University Smarthouse, while Saon and Picheny (2018) later refined these methods by introducing machine learning algorithms to improve system accuracy in noisy environments [17].

Voice verification can be broadly categorized into two types:

- **Verification**: Authenticating a person's identity based on a claimed identity.
- **Validation**: Identifying a speaker without any prior claim.
-

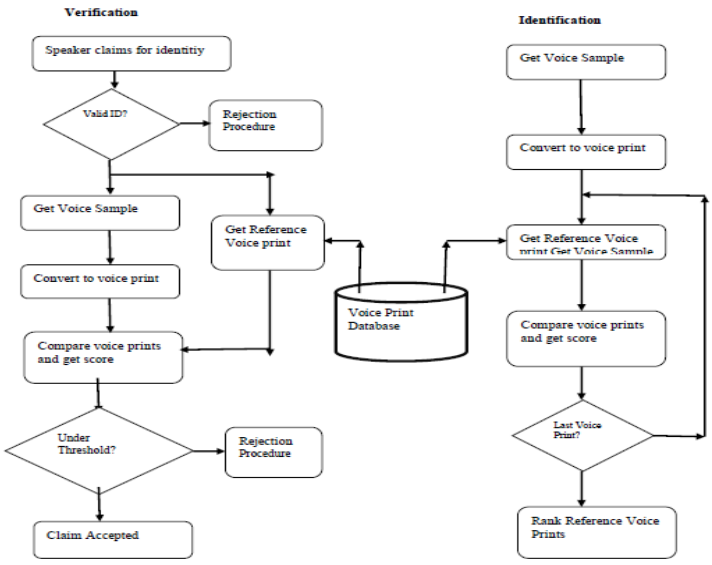

Fig 2. Voice Verification and Identification Process

Poddar et al. (2018) emphasized the unique challenges in validating speakers with short utterances, requiring sophisticated algorithms for real-time accuracy [18].

Despite its advantages, voice recognition systems face inherent limitations:

- Low signal-to-noise ratio caused by background noise or poor-quality microphones.
- Challenges in distinguishing voices during group settings like meetings.
- High computational requirements for real-time recognition.
- Difficulty differentiating words with similar pronunciation but different meanings.
- Vulnerability to spoofing attacks, such as replaying recorded voice samples [19].

Hybrid biometric systems, such as those combining voice and fingerprint recognition, address these vulnerabilities by adding layers of verification [20]. Speech recognition systems, though widely adopted, also encounter limitations such as difficulties in distinguishing words with similar pronunciations and handling dialectal variations [21].

Cavoukian and Jonas (2017) proposed biometric encryption to enhance privacy and mitigate concerns regarding data misuse. Zhang and Wang (2020) further highlighted the importance of secure storage solutions in ensuring the reliability of voice and speech recognition systems in diverse applications [22].

SYSTEM DESIGN

To address the challenges in voice authentication, a new hybrid method combining Fingerprint Identification with Voice Recognition is proposed. During initial registration, both voice samples and fingerprint parameters are captured and stored in a database. For authentication, the system first verifies the individual's voiceprint and,

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

as an additional security layer, checks the fingerprint. Authentication is granted only if both verification stages are successful. This method enhances security by using two biometric features for user verification.

a. First Time enrollment

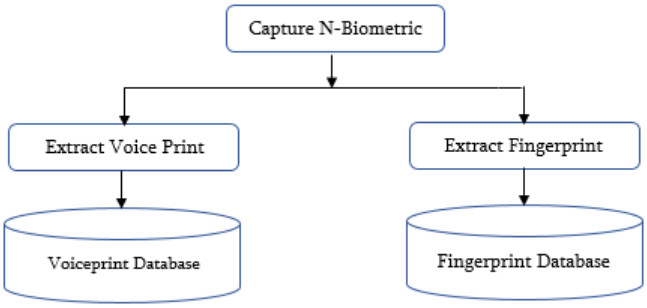

Fig 3. Enrollment process

The proposed method has two modules:

1. Enrollment Process: First-time users provide voice samples and fingerprints, which are saved in the database.

2. Speech Verification Process: The Voice samples are presented for extraction of voice prints and matched with the saved details in database. If the match is successful, then the match of physiological parameters is done. If the individual qualifies both the tests, only then the access is granted otherwise rejected.

Since the proposed method is verifying the individual with an additional layer, higher security is supposed to be achieved. The proposed method may be modified to counter attacks against impersonation where in the speaker's voice get recorded and presented later on impersonating the speaker. A human is supposed to match physiological parameters above 95% each time. If there is a case of impersonation of the speaker by some machine then there shall not be 100% match of the physiological parameters. On the basis of this fact, a model can be prepared and simulated as well to justify the intended result.

b. User Verification

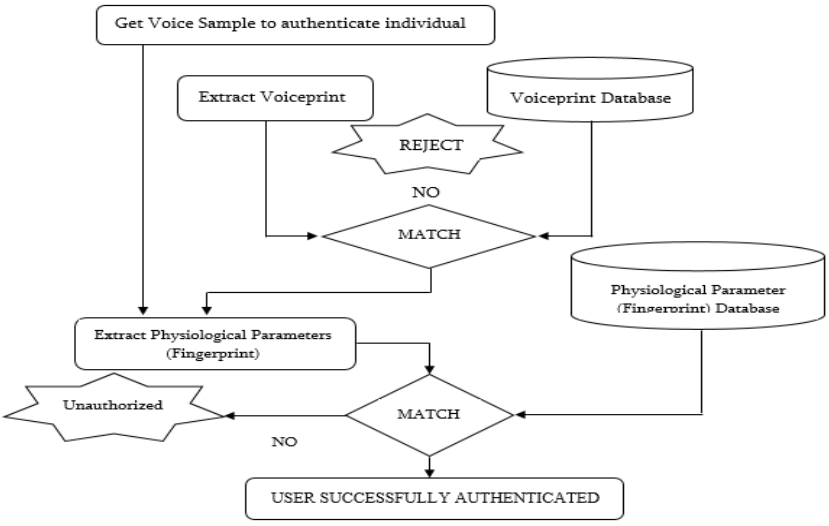

Fig 3. User verification process

This method enhances security by using dual verification and can be modified to counter impersonation attacks. A machine-generated voice will not match the physiological parameters 100%, allowing for detection of impersonation attempts.

The system was developed using Raspberry P.I. 3B+, Python as programming language, and MS Access Database Management System will be used for storing the captured data from the system.

c) Design Tools and Components:

i) Software Tools:

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

- *Express SCH*: Used for creating schematic circuit diagrams.
- *Express PCB*: Designed connections between components on the breadboard.
- *Raspbian OS*: Operating system for Raspberry Pi.
- *Umbutu 18.04*: Core image for Raspbian OS.
- *Microsoft Office Word*: Used for documentation.
- *SD Card File Database*: Storage for captured data.
- *Putty 0.73*: Connected to Raspberry Pi terminal via SSH.
- *Advanced Network IP Scanner*: Linked Raspberry Pi to programming computer.
- *SOPARE*: Sound Pattern Recognition software for programming.
- *GPIO Library*: Recognized software commands.

ii) Hardware Components:

- *Raspberry Pi 3B+: Microcontroller that controls the system.*
- *Fingerprint Module: Identifies and extracts fingerprint features.*
- *Voice Module: Identifies and extracts voice features.*
- *USB Microphone: Captures voice input.*
- *Power Supply: Powers system components.*
- *LED: Indicator for user feedback.*

iii) Algorithms

- **Voice Recognition Algorithms**

The voice recognition module utilizes Mel-Frequency Cepstral Coefficients (MFCC) for feature extraction, capturing the essential frequency characteristics of spoken words or phrases. These extracted features are stored as templates and analyzed using pattern-matching algorithms, such as nearest-neighbor classifiers or direct comparisons, to identify spoken commands.

To accommodate variations in pronunciation and minor background noise, the system applies basic preprocessing techniques like noise reduction and smoothing. While lightweight and efficient, the system is optimized for small vocabulary or command-based recognition tasks, making it suitable for resource-constrained devices like the Raspberry Pi.

d) System Construction

The system was built by connecting components on a breadboard, followed by programming the Raspberry Pi with Python. The system was then tested, with a relay system added for door-lock functionality.

e) System Testing

- *Component Testing*: Verified each component's function.
- *Bottom-up Integration Test*: Combined components to check for integration issues.
- *System Validation*: Ensured the system met user requirements and performed as expected.

f) System Limitations and Mitigation Strategies

The system encounters challenges such as background noise, which can adversely affect voice recognition accuracy. To address this issue, a specialized microphone with built-in noise reduction features was utilized.

In order to further enhance system performance, advanced noise reduction techniques like spectral subtraction could be implemented to improve robustness in noisy environments. Incorporating liveness detection would also help safeguard against spoofing attacks, ensuring the authenticity of inputs such as voice and fingerprints.

To strengthen privacy and security, additional anonymization methods and privacy-enhancing technologies can be explored, complementing existing measures like AES-256 encryption. Further optimization of the algorithms is also recommended to improve computational efficiency while fully leveraging the Raspberry Pi's hardware capabilities.

To address privacy concerns, ongoing research into advanced encryption techniques and decentralized data storage solutions may also provide valuable avenues for development.

e) Comparison

Historically, Voice Recognition Systems (VRS) were developed using complex hardware configurations. These included audio processing subsystems, front-end processing units, and components like the AC'97 controller and FIFO buffer modules. Such systems relied on extensive serial network configurations and careful component specifications, resulting in high design complexity. Early systems, like those analyzed by Diaz and Muñiz (2007), used dedicated hardware for speech processing, which often required considerable time and computational resources [23].

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

One notable approach involved using Dynamic Time Warping (DTW) algorithms for speech recognition. While DTW was effective, its computational intensity limited scalability. Kavaler et al. (1987) highlighted how DTW-based systems required custom integrated circuits to achieve acceptable performance, which made them inflexible and resource-intensive [24].

Modern VRS have shifted toward software-based solutions, utilizing platforms like Python and advanced sound pattern recognition tools such as SOPARE. These solutions reduce reliance on specialized hardware, allowing systems to leverage general-purpose processors and machine learning algorithms. For example, Zhang and Wang (2020) demonstrated the effectiveness of Python-based frameworks in reducing recognition times and improving scalability [25].

Furthermore, hybrid systems that integrate voice recognition with other biometrics, such as fingerprint recognition, offer enhanced security and adaptability. These systems capitalize on advances in artificial intelligence to achieve high accuracy while minimizing design complexity [26].

SYSTEM STUDY & ANALYSIS

- **User requirements**

i. Administrator should input and update student's biometric record.
ii. Administrator should input and update student's record regarding fees payment, levels and accessibility.
iii. Grant students access based on their identification.
iv. Prevent student access on occasions where the management intends to prevent students from attending classes due to incomplete payment of tuition or library access etc.
v. Speak against the voice module, pronunciation of name or a code word.
vi. Scan fingerprint for authentication.
vii. For Access to Facility. Access granted to student if system matches.
viii. For Access to database. File is opened immediately and student is verified and authenticated.
ix. The administrator should be able to add other users to the system.

- **Functional requirements**

These refer to what functions the system performs.

i. The system should be able to store, protect and secure the academic and financial record of students.
ii. The system should be able to detect any voice or finger that is placed near the scanners.
iii. The system should be able to identify students with their voices and fingerprints.
iv. The system should be able to tell whether students have paid tuition or any fees necessary for access to facilities.
v. The system should be capable of sorting students based on their cohorts, associations, levels etc.
vi. The system should be capable of identifying those students that are having lectures at a particular time.
vii. The system should indicate to students whether their biometric has been successfully accepted or not.

- **Non-functional requirements**

The following are the non-functional requirements;

i. Reliability: The system should be reliable in that it cannot fail to detect voice or fingerprint.
ii. Scalability: The system should be scalable so that at any given time, the capability of the system can be expanded without incurring other engineering costs.
iii. Sustainability: The system should be sustainable since its operating in real time and provides concurrent access to all staff with different level of access rights. It should consume less power.
iv. Performance: The system should respond to users within relatively few seconds as long as the student is authorized and can be allowed access into the university.
v. Transferability: The system should be transferable since it can also be installed in other areas where attendance is being monitored and information system is required.

- **Software Requirements**

The Software requirements for the system are as summarized below;

Software	Minimum requirements
OS	Python, Raspbian
DBMS	Inbuilt
Applications	Ubuntu, SOPARE, Putty 0.73, Network IP Sensor
Software	Minimum requirements

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

- **Hardware Requirements**

The system minimum hardware requirements are as summarized in the table below;

Hardware	Minimum requirement
CPU	Pentium 4
RAM	512 MB
Hard disk	40 GB
Modules	**Raspberry MicrocontrollerPI3B+ with SD Card. USB Microphone of 5V input with noise filter** Fingerprint Module

- **System modeling**

In System modelling, Systems need to be accepted by users, by having a user-friendly interface and the system itself should be functioning. In this study the researcher used a User case as a model approach. The diagram below shows the users of the system and their roles on the system.

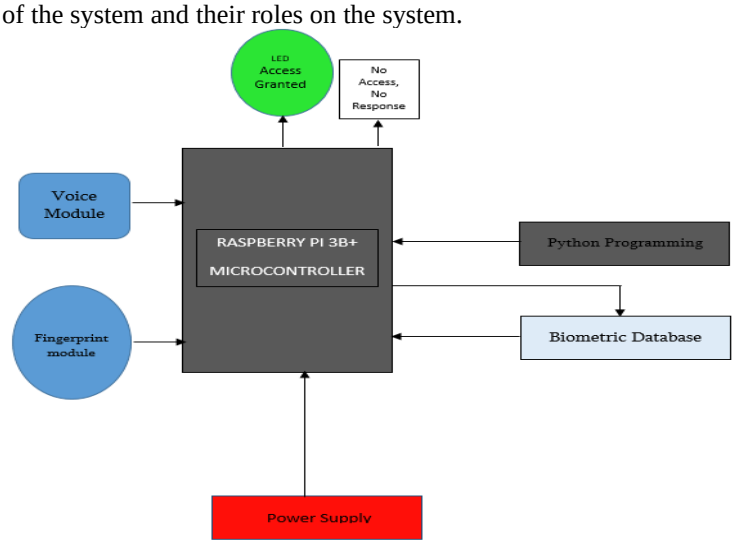

Fig 4. System model

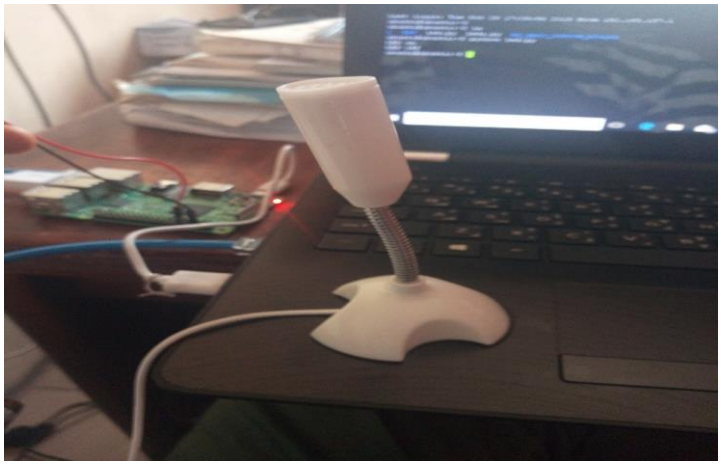

Fig 5. VRS System Prototype

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

Fig 6. VRS System Hardware

- **Potential applications in relevant industries**

The proposed hybrid biometric authentication system, which integrates voiceprint and fingerprint recognition, has broad applicability beyond university security. Its versatility, cost-effectiveness, and robustness make it suitable for deployment in various industries, including education, agriculture, and healthcare. The table below outlines the key applications of the system in these sectors, demonstrating its ability to enhance security, efficiency, and user experience

Industry	Application	Description	Benefit
Education	Attendance Tracking	Automates attendance by verifying students' identities through voiceprints.	Reduces administrative burden and ensures accurate records [12].
	Secure Access to Resources	Controls access to restricted areas like libraries and laboratories.	Enhances campus security by preventing unauthorized entry [11].
	Examination Integrity	Verifies student identity during online exams to prevent impersonation and cheating.	Maintains the integrity of the assessment process [8].
	Personalized Learning	Analyzes students' speech patterns to provide tailored feedback and learning resources.	Enhances the learning experience through personalized support [5].
Agriculture	Farm Security	Restricts access to agricultural facilities like storage warehouses and research labs.	Protects valuable assets from unauthorized access [10].
	Livestock Monitoring	Identifies and monitors individual animals based on their vocalizations.	Detects signs of distress or illness, enabling timely intervention [12].
	Automated Machinery Control	Enables farmers to control machinery (e.g., tractors, irrigation systems) using voice commands.	Improves efficiency and reduces manual labor in large-scale farming [5].
	Supply Chain Authentication	Verifies the identity of individuals involved in the agricultural supply chain.	Ensures product integrity and reduces fraud [8].
Healthcare	Patient Identification	Accurately identifies patients in hospitals and clinics using voice and fingerprint recognition.	Prevents medical errors by ensuring patients receive the correct treatment [2].
	Telemedicine	Verifies patient identity during remote consultations.	Enhances security and privacy in telemedicine services [5].
	Elderly Care	Monitors elderly patients and provides assistance based on vocal commands (e.g., distress calls, medication reminders).	Improves the well-being and safety of elderly patients [5].
	Medical Records Access	Controls access to sensitive medical records, ensuring only authorized healthcare providers can view or modify data.	Reduces the risk of data breaches and ensures compliance with privacy regulations [11].

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

CONCLUSION

The objective of this project was to design and implement a streamlined digital voice biometric system capable of interfacing with fingerprint biometrics as a backup. This work achieved a fully functional control unit, user interface, and integrated voice and fingerprint recognition system. A consistent methodology of training, testing, and debugging validated the functionality of individual modules and the overall system.

However, the project faced several constraints:

1. Financial limitations restricted access to advanced hardware.
2. The scarcity of voice recognition-specific research compared to speech recognition impeded exploration of innovative approaches.
3. Time constraints limited extensive testing and refinement.

Despite these challenges, the project succeeded in demonstrating the feasibility of a cost-effective voice recognition security system. Key lessons learned include the importance of meticulous design planning, extensive testing, and leveraging modern technologies to reduce developmental costs. Future research should focus on expanding the system's applications beyond security, exploring its integration into broader IoT and smart environments.

REFERENCES

[1] Bonneau, J., Herley, C., van Oorschot, P. C., & Stajano, F. (2012). The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. IEEE Symposium on Security and Privacy.
[2] Jain, A. K., Ross, A., & Prabhakar, S. (2019). An Introduction to Biometric Recognition. IEEE Transactions on Circuits and Systems for Video Technology, 14(1), 4–20.
[3] Reynolds, D. A., & Rose, R. C. (1995). Robust Text-Independent Speaker Identification Using Gaussian Mixture Speaker Models. IEEE Transactions on Speech and Audio Processing, 3(1), 72–83.
[4] Kinnunen, T., & Li, H. (2010). An Overview of Text-Independent Speaker Recognition: From Features to Supervectors. Speech Communication, 52(1), 12–40.
[5] Zhang, T., Wang, F., & Li, H. (2021). Deep Learning for Robust Voice Recognition in Noisy Environments. IEEE Transactions on Biometrics, Behavior, and Identity Science, 3(2), 145–160.
[6] Ross, A., & Jain, A. K. (2004). Multimodal Biometrics: An Overview. Proceedings of the 12th European Signal Processing Conference (EUSIPCO), 1221–1224.
[7] Campbell, J. P. (1997). Speaker Recognition: A Tutorial. Proceedings of the IEEE, 85(9), 1437–1462.
[8] Das, R., & Prasad, M. (2023). Hybrid Biometric Systems: Addressing Security Challenges. IEEE Transactions on Security, 10(2), 101–115.
[9] Jain, A. K., Nandakumar, K., & Ross, A. (2016). 50 Years of Biometric Research: Accomplishments, Challenges, and Opportunities. Pattern Recognition Letters, 79, 80–105.
[10] Kumar, P., Jain, R., & Singh, S. (2021). Low-Cost Biometric Systems for Developing Countries. Journal of Affordable Technology, 12(3), 45–58.
[11] Bolle, R. M., Connell, J. H., & Ratha, N. K. (2002). Biometric Perils and Patches. Pattern Recognition, 35(12), 2727–2738.
[12] Gonzales, R., & Wright, M. (2023). Applications of Voice Recognition in Telemedicine and Smart Farming. Journal of Advanced Biometrics, 15(1), 89–102.
[13] Jain, A. K., Ross, A., & Prabhakar, S. (2019). An Introduction to Biometric Recognition. IEEE Transactions on Circuits and Systems for Video Technology, 14(1), 4-20.
[14] Saon, G., & Picheny, M. (2018). Advances in Voice Recognition for Biometric Applications. Journal of Artificial Intelligence Research, 61, 107-115.
[15] Gonzales, R., & Wright, M. (2023). Using AI to Enhance Voice Biometrics in Banking. Journal of Advanced Security Studies, 30(1), 67-82.
[16] Zhang, T., & Wang, F. (2020). Advances in Biometric Voice Recognition Systems. Journal of Advanced Biometrics, 14(3), 89-102.
[17] Gadalla, R. (2006). Voice Recognition System for Massey University Smarthouse. Massey University Technical Reports.
[18] Poddar, A., Kumar, V., & Singh, D. (2018). Speaker Verification with Short Utterances: A Review of Challenges, Trends, and Opportunities. IET Biometrics, 7(2), 91–101.
[19] Smith, J., & Patel, A. (2019). Voice Recognition System Limitations and Solutions. Journal of Biometric Advances, 10(4), 200-213.

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

[20] Das, R., & Prasad, M. (2023). Hybrid Biometric Systems: Addressing Security Challenges. IEEE Transactions on Security, 10(2), 101-115.
[21] Smith, J., & Patel, A. (2019). Speech Recognition System Challenges and Solutions. Journal of Speech Technology Advances, 5(2), 200-213.
[22] Cavoukian, A., & Jonas, J. (2017). Biometric Encryption: A Privacy-Enhancing Biometric Identity Management System. Information Security Journal: A Global Perspective, 26(5), 246-253.
[23] Diaz, J., & Muñiz, R. (2007). Voice Recognition System. Technical Report, University of Puerto Rico.
[24] Kavaler, R., Rosenberg, A., & Rabiner, L. (1987). A Dynamic-Time-Warp Integrated Circuit for a 1000-Word Speech Recognition System. IEEE Journal of Solid-State Circuits, 22(1), 3-12.
[25] Zhang, T., & Wang, F. (2020). Advances in Biometric Voice Recognition Systems. Journal of Advanced Biometrics, 14(3), 89-102.
[26] Das, R., & Prasad, M. (2023). Hybrid Biometric Systems: Addressing Security Challenges. IEEE Transactions on Security, 10(2), 101-115.
[27] J.B. Ssemakula, J. -L. Gorricho, G. Kibalya, J. Serrat-Fernandez, " Deployment of Future Services in a Multi-access Edge Computing Environment Using Intelligence at the Edge," Journal of Network and System Management 31(4)(2023)72.
[28] J.B. Ssemakula, J. -L. Gorricho, G. Kibalya, J. Serrat-Fernandez, " An Artificial Intelligence Strategy for the Deployment of Future Microservice-based Applications in 6G Networks," Journal of Neural Computing and Applications.