International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
© 2026 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

Research Paper

A NOVEL DIGITAL AUDIO ENCRYTION AND WATERMARKING SCHEME

SHAGAM GEETHA [1], CHAPPIDI SATHWIKA [2], DORAPALLY SRIHARIKA [3], RISHIK MADURI [4], YARABANDLA YASHWANTH REDDY [5]

[1]Assistant Professor, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

[2, 3, 4, 5] B.Tech, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

ABSTRACT— To enhance the privacy and security of audio signals stored in third-party storage centers, a robust digital audio encryption and forensics watermarking scheme is proposed. The scheme incorporates the AES-GCM (Advanced Encryption Standard in Galois/Counter Mode) algorithm for authenticated encryption, ensuring both confidentiality and integrity of the audio data. In addition, we utilize Fernet symmetric encryption and PBKDF2HMAC (Password-Based Key Derivation Function 2 with HMAC) for key generation, supported by generative hash passwords to further strengthen security. The signal energy ratio feature of audio signals is defined and used in the watermark embedding method through feature quantification, improving the resilience of the watermarking system. First, the original audio is encrypted using scrambling, multiplication, and AES-GCM to generate the encrypted data. The encrypted data is then divided into frames, each compressed through sampling. The compressed data, along with frame numbers, is embedded into the encrypted audio, forming the watermarked signal which is uploaded to third-party storage. Authorized users retrieve the encrypted data and verify its authenticity. If intact, the data is decrypted directly using Fernet to recover the original audio. In the case of an attack, the compromised frames are identified, and the embedded compressed data is used to reconstruct the audio approximately. The reconstructed signal is subsequently decrypted to retain the expression meaning of the original audio.

Experimental results demonstrate the effectiveness of the proposed scheme in providing quantum-safe encryption, secure watermarking, and forensics capabilities.

Index Terms – Audio encryption, AES-GCM, Fernet encryption, PBKDF2HMAC, digital watermarking, audio forensics, authenticated encryption, signal integrity, quantum-safe security, secure cloud storage, audio authentication, cryptography.

I. INTRODUCTION

In today's digital landscape, the storage and sharing of audio signals have become commonplace, raising significant concerns about privacy, security, and data integrity. As audio content is increasingly stored in third-party storage centers, the risks of unauthorized access, data tampering, and potential data loss intensify, necessitating robust security measures. To address these challenges, we propose a comprehensive digital audio encryption and forensics watermarking scheme that combines advanced cryptographic techniques to ensure the confidentiality and integrity of audio data. Central to our approach is the implementation of the AES-GCM (Advanced Encryption Standard in Galois/Counter Mode) algorithm, which not only provides strong encryption but also incorporates authentication mechanisms, ensuring that the audio data remains protected against both unauthorized access and tampering. To further enhance security, we employ Fernet symmetric encryption along with PBKDF2HMAC (Password-Based Key Derivation Function 2 with HMAC) for key generation, leveraging generative hash passwords to establish a secure framework for managing encryption keys. Our methodology involves a multi-step process where the original audio is first encrypted using techniques such as scrambling, multiplication, and AES-GCM, resulting in a secure encrypted data stream. This data is then segmented into frames, which are compressed through sampling, allowing for efficient storage and processing. The compressed data, accompanied by frame numbers, is subsequently embedded into the encrypted audio, resulting in a watermarked signal that can be safely uploaded to third-party storage. This comprehensive scheme not only enables authorized users to retrieve and verify the authenticity of the encrypted data but also ensures that, in the event of an attack, any compromised frames can be identified and reconstructed. The embedded compressed data plays a critical role in this reconstruction process, enabling the

approximate recovery of the original audio signal, which is then decrypted to preserve its expressive meaning. Through rigorous experimental validation, our proposed scheme demonstrates its effectiveness in providing quantum-safe encryption, secure watermarking, and robust forensics capabilities, ultimately contributing to a more secure and trustworthy digital audio environment.

II. RELATED WORK

A. *Quantum-Safe Audio Encryption: Challenges and Solutions*

This paper investigates the vulnerabilities of traditional audio encryption algorithms in the face of quantum computing advancements. It highlights the impact of quantum algorithms, such as Shor's algorithm, on widely-used audio encryption methods like Advanced Encryption Standard (AES) and the Rivest-Shamir-Adleman (RSA) algorithm. The authors discuss several quantum-safe alternatives for audio encryption, including lattice-based cryptography, code-based cryptography, and multivariate polynomial systems. A key focus of the study is the adaptation of these quantum-safe algorithms to the specific requirements of audio data protection, addressing issues like low latency and efficient processing. The paper also explores the integration of hybrid cryptographic systems that combine quantum-safe methods with classical encryption to ensure backward compatibility and gradual transition. The results suggest a roadmap for securing audio communications in the post-quantum era.

B. *Performance Evaluation of Quantum-Safe Algorithms for Audio Encryption*

This paper presents a comprehensive performance evaluation of several quantum-safe encryption algorithms specifically designed for audio encryption. The authors compare lattice-based and hash-based cryptographic systems in terms of encryption and decryption speed, computational resources required, and robustness against quantum attacks. Through simulations using different audio datasets, the paper demonstrates the trade-offs between security and performance, emphasizing the importance of real-time processing capabilities in audio applications. The study also explores the potential for hybrid encryption models that combine quantum-safe algorithms with conventional encryption techniques to improve performance in large-scale audio communication systems. Insights into the challenges and future developments of quantum-safe audio encryption are also provided.

C. *Post-Quantum Cryptography for Audio Communications: A Survey*

This survey provides an in-depth analysis of post-quantum cryptographic techniques that can secure audio communications in the face of emerging quantum threats. The authors review a variety of encryption schemes, including lattice-based, hash-based, and code-based algorithms, and assess their applicability to the protection of audio data. The paper also discusses the specific challenges of implementing these cryptographic solutions for audio, such as low power consumption and minimal computational overhead. Case studies and real-world examples are provided to highlight the effectiveness of these techniques in securing audio files and voice communications in environments vulnerable to quantum attacks. The authors also propose hybrid encryption models that combine quantum-safe algorithms with existing cryptographic standards to ensure a smooth transition to post-quantum systems.

D. *Quantum-Safe Audio Transmission: A Comparative Study of Encryption Techniques*

This paper compares a range of quantum-safe encryption techniques tailored for audio transmission over unsecured channels. The authors assess the performance and security of several post-quantum cryptographic algorithms, including lattice-based cryptography and multivariate quadratic polynomials, focusing on their application to encrypted audio communication. Special attention is given to the challenges of adapting these techniques to audio streams, such as minimizing delay and maintaining sound quality. The paper also evaluates how these algorithms can be incorporated into existing secure communication frameworks, proposing solutions to overcome implementation challenges. Finally, the authors present a set of recommendations for selecting the most suitable encryption algorithms based on different audio transmission requirements.

III. PROPOSED METHODOLOGY

Enhanced Encryption with AES-GCM(Advanced Encryption Standard in Galois/Counter Mode) and Fernet is the proposed system replaces the traditional encryption methods with AES-GCM (Advanced Encryption Standard - Galois/Counter Mode) for authenticated encryption, ensuring data confidentiality and integrity. Additionally, Fernet encryption is used to securely encrypt and decrypt the audio data, ensuring that any unauthorized tampering with the data can be detected.

PBKDF2HMAC (Password-Based Key Derivation Function 2 with HMAC) is employed to derive strong encryption keys from passwords using generative hash passwords, further strengthening the security of the system. Additionally, Discrete Wavelet Transform (DWT) has gained popularity in watermarking schemes due to its ability to represent signals at multiple resolutions. The DWT decomposes the audio signal into a set of coefficients that represent different frequency subbands, making it well-suited for embedding watermark data. DWT coefficients offer better localization in both time and frequency domains compared to DFT, which improves the robustness of the watermark against various attacks such as compression, noise, and resampling. This multi-resolution analysis provided by DWT enables more flexible and secure watermarking techniques while maintaining audio fidelity.

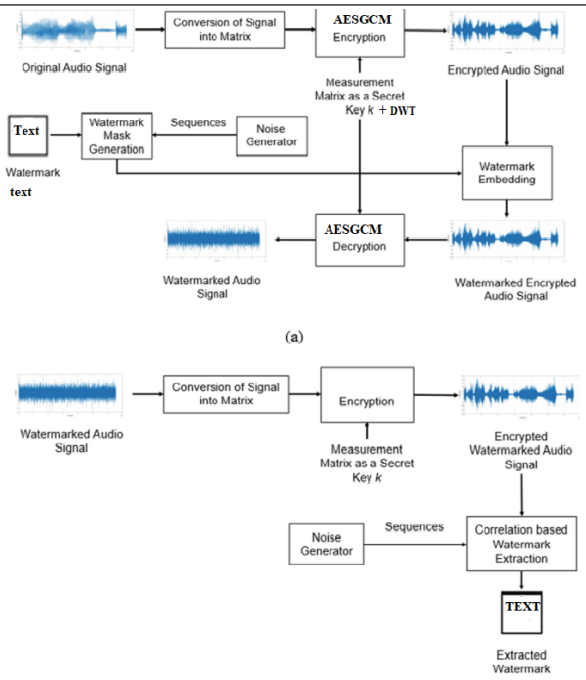

Fig. 1: System Overview

1. Cryptography

The application employs the cryptography library to implement secure audio encryption and decryption.

2. Fernet Encryption

The Fernet class provides symmetric encryption. The generate_key function derives a secure key from a password using the PBKDF2HMAC algorithm, ensuring that the encryption keys are strong and resistant to brute-force attacks.

3. AES-GCM (Advanced Encryption Standard - Galois/Counter Mode)

This is used for authenticated encryption, providing both confidentiality and integrity

of the audio data. The application uses this mode to encrypt audio files while embedding a watermark.

4. PBKDF2HMAC

This cryptographic function is part of the cryptography library and is used for deriving encryption keys from passwords. It applies a hash function (SHA-256) along with a salt and multiple iterations to create a secure key, enhancing resistance to dictionary and brute-force attacks. This makes user-provided passwords much more secure when generating encryption keys.

5. Base64

The application utilizes base64 encoding to convert binary data (like encryption keys) into a string format that can be easily stored or transmitted.

This is particularly useful for representing keys in a URL-safe manner when embedding them in web applications.

6. Try-Except Blocks

The application employs error handling through try-except blocks in critical functions like encrypt_audio and decrypt_audio.

This ensures that any exceptions raised during file operations, encryption, or decryption processes are caught, allowing the application to provide user-friendly feedback without crashing.

7. Watermarking Logic

The encrypt_audio function incorporates watermarking by appending a watermark string to the audio frames before encryption.

This is a simplistic approach to watermarking; however, it demonstrates the application's capability to embed additional information into audio files, which can later be extracted during decryption.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

The experimental results show that the proposed digital audio encryption and watermarking scheme effectively ensures confidentiality, integrity, and authentication of audio signals. The combination of AES-GCM, Fernet encryption, and PBKDF2HMAC provides strong encryption and secure key management, while the watermarking technique enables reliable tamper detection and forensic recovery. The system successfully reconstructs compromised audio frames after attacks, preserving the original audio content.

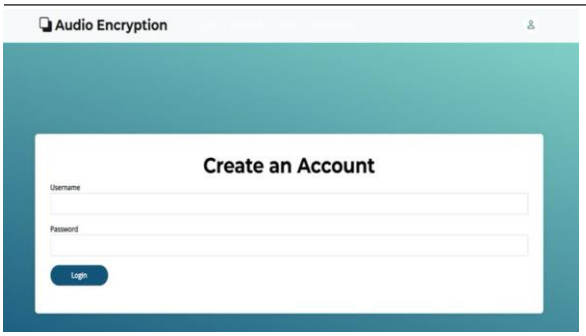

Fig. 2: Create Account

Fig. 3: Dashboard

Fig. 4: Encrypt Audio

Fig. 5: Decrypt Audio

V. CONCLUSION

In conclusion, this Flask application serves as a robust solution for secure audio file management, effectively integrating encryption, watermarking, and user authentication features. By leveraging advanced cryptographic techniques such as AES-GCM and Fernet for encryption, along with innovative watermarking methods, the application ensures the confidentiality and integrity of audio data while allowing users to embed and retrieve watermarks seamlessly. The modular architecture not only promotes maintainability and scalability but also provides a foundation for future enhancements, such as improved user management and advanced audio processing capabilities. As the digital landscape continues to evolve, this application stands poised to meet the growing demands for secure audio file handling, making it a valuable tool for both casual users and professionals in the field. Through continuous development and adaptation, it aims to provide an unparalleled user experience while maintaining the highest standards of security and functionality in audio file management.

REFERENCES

[1] R. Giampiccolo, A. Bernardini, and A. Sarti, ‘‘Wave digital models of piezoelectric transducers for audio applications,’’ IEEE Sensors J., vol. 23, no. 1, pp. 389–400, Jan. 2023.

[2] F. S. Mobley, G. Bowers, M. Ugolini, E. Fox, and N. Gillespie, ‘‘Modeling aircraft similarity with musical auditory feature extraction,’’ Appl. Acoust., vol. 214, Nov. 2023, Art. no. 109689.

[3] H.-T. Hu, H.-H. Chou, and T.-T. Lee, ‘‘Robust blind speech watermarking via FFT-based perceptual vector norm modulation with frame selfsynchronization,’’ IEEE Access, vol. 9, pp. 9916–9925, 2021.

[4] Z. Liu, Y. Huang, and J. Huang, ‘‘Patchwork-based audio watermarking robust against de-synchronization and recapturing attacks,’’ IEEE Trans. Inf. Forensics Security, vol. 14, no. 5, pp. 1171–1180, May 2019.

[5] G. Zhang, L. Zheng, Z. Su, Y. Zeng, and G. Wang, ‘‘M-sequences and sliding window based audio watermarking robust against largescale cropping attacks,’’ IEEE Trans. Inf. Forensics Security, vol. 18, pp. 1182–1195, 2023.

[6] H. Liu, ‘‘Audio block encryption using 3D chaotic system with adaptive parameter perturbation,’’ Multimedia Tools Appl., vol. 82, no. 18, pp. 27973–27987, Jul. 2023.

[7] A. Kumar and M. Dua, ‘‘Audio encryption using two chaotic map based dynamic diffusion and double DNA encoding,’’ Appl. Acoust., vol. 203, Feb. 2023, Art. no. 109196.

[8] B. Rahul, K. Kuppusamy, and A. Senthilrajan, ‘‘Chaos-based audio encryption algorithm using biometric image and SHA-256 hash algorithm,’’ Multimedia Tools Appl., vol. 82, no. 28, pp. 43729–43758, Nov. 2023.

[9] E. A. Albahrani, T. K. Alshekly, and S. H. Lafta, ‘‘New secure and efficient substitution and permutation method for audio encryption algorithm,’’ J. Supercomput., vol. 79, no. 15, pp. 16616–16646, Oct. 2023.

[10] A. S. Alanazi, N. Munir, M. Khan, and I. Hussain, ‘‘A novel design of audio signals encryption with substitution permutation network based on the genesio-tesi chaotic system,’’ Multimedia Tools Appl., vol. 82, no. 17, pp. 26577–26593, Jul. 2023

AUTHORS Profile

Mrs. SHAGAM GEETHA has received her B.Tech in 2012 from Nagarjuna Institute of Technology, JNTUH. She completed her M.Tech in Computer Science and Engineering (CSE) in 2014 from Vidya Vikas Institute of Technology, JNTUH.

Ms. CHAPPIDI SATHWIKA pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.

Ms. DORAPALLY SRIHARIKA pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Tech-nical Campus affiliated to JNTUH in 2022-2026.

Mr. RISHIK MADURI pursuing B. Tech degree in Computer Science and Engine-ering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.

Mr. YARABANDLA YASHWANTH REDDY pursuing B. Tech degree in Computer Science and Engine-ering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.