International Journal of Scientific Research in Engineering and Management (IJSREM)
Special Edition - Volume 09 NCFT -2025 SJIF Rating: 8.586 ISSN: 2582-3930

A Novel Digital Audio Encryption and Watermarking Scheme

1st M Venkatesh
Department of CSE
GNITC, Hyderabad.

2nd Kesari Rahul
Department of CSE
GNITC, Hyderabad.

3rd K Pranith Reddy
Department of CSE
GNITC, Hyderabad.

4th K Vijaya
Department of CSE
GNITC, Hyderabad.

5th Suruchi W. Kitey
Department of CSE
GNITC, Hyderabad.

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.

Keywords: Audio Encryption, Watermarking, AES-GCM, Fernet, PBKDF2HMAC, DWT, Signal Energy Ratio, Cybersecurity.

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 theconfidentiality 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.

A. Scope of the project

The scope of the proposed digital audio encryption and forensics watermarking scheme encompasses critical areas essential for addressing contemporary challenges in audio data security, privacy, and integrity. Primarily, it aims to protect audio signals stored in third-party storage centers from unauthorized access and potential data breaches through advanced encryption techniques such as AES-GCM, ensuring that only authorized users can decrypt and access original content. The integration of authentication mechanisms guarantees data integrity, allowing users to verify the authenticity of audio files, which is particularly crucial in sensitive environments like legal or medical recordings. Furthermore, the scheme enhances watermarking resilience against various attacks, embedding information that remains intact under adverse conditions, thereby facilitating effective tracking and copyright protection. With robust forensic capabilities, the method allows for identifying and reconstructing compromised audio frames, enabling approximate recovery of the original signal in case of an attack. The focus on quantum- safe encryption methods positions the scheme as a forward-thinking solution that safeguards sensitive information against future advancements in computing power.

II. NEED OF THE STUDY

In the digital era, audio data is increasingly used for communication, media, surveillance, education, and legal evidence. With the rapid growth of **cloud computing and third-party storage platforms**, protecting this sensitive data from **unauthorized access, tampering, and piracy** has become a major concern. Traditional encryption and watermarking systems are no longer sufficient to meet the security demands of today's data-driven environments. This creates a **strong need to study and develop advanced techniques** for secure audio handling.
Here's why this study is essential:

1. Increasing Security Threats to Audio Data
Audio files can be **intercepted, modified, or copied** without authorization, leading to **data breaches, forgery, and misuse**. Conventional encryption methods secure data but **cannot detect tampering or recover compromised content**, making enhanced techniques necessary.

2. Lack of Authentication and Tamper Detection in Existing Systems
Most traditional systems focus only on encryption, ignoring the **integrity and authenticity** of the audio. If an attacker alters the file, there's **no way to detect or prove** the modification. Hence, there's a need for **authenticated encryption and forensic watermarking** to track and verify changes.

3. Inadequate Recovery Mechanisms
When audio data is damaged or attacked, **existing systems fail to recover the original content**, leading to **data loss or loss of meaning**. This project introduces **embedded compressed data** as a watermark to enable **partial or full reconstruction**, highlighting the need for **recovery-focused audio security**.

4. Legal and Forensic Applications
In law enforcement and legal proceedings, audio data may serve as **evidence**. The ability to **prove ownership, detect tampering, and restore original meaning** is essential. This study addresses the **forensic requirements** of modern audio systems.

5. Rising Threat from Quantum Computing
As **quantum computers** become more capable, traditional cryptographic methods like RSA and ECC will become obsolete. There's a need to **future-proof audio encryption** using **quantum-safe algorithms** such as AES-GCM and PBKDF2HMAC, as done in this project.

6. Protection of Intellectual Property
With the rise of music, podcasts, and digital media, protecting audio from **unauthorized copying and distribution** is vital. **Watermarking ensures traceability and copyright protection**, making it an essential part of digital content security.

7. Efficiency and Storage Optimization
Audio files often take up **significant storage space**. By incorporating **frame-based compression** before watermark embedding, the project addresses both **security and storage efficiency**, which is critical for large-scale cloud-based applications.

III. Existing System

Most traditional audio watermarking systems employ DFT(Discrete Fourier Transform) to transform signals from the time to frequency domain, where watermark data can be embedded into frequency coefficients. These methods maintain audio fidelity while hiding data imperceptibly. However, DFT-based techniques are sensitive to signal processing operations like noise addition, resampling, and lossy compression. Moreover, such approaches generally lack

robust authentication mechanisms and rely on simple or outdated encryption techniques.

Limitations of the existing approaches include:
- High vulnerability to signal degradation.
- Minimal support for tamper detection or error correction.
- Lack of forward-compatibility with post-quantum cryptographic standards.

IV. Proposed System

The proposed system addresses these shortcomings through a fusion of cryptographic and signal processing strategies. AES-GCM provides authenticated encryption, ensuring that both the confidentiality and integrity of the audio are preserved. Fernet encryption introduces another layer of symmetric encryption that is easy to implement and quantum-safe. PBKDF2HMAC is utilized to derive secure keys from user-provided passwords by applying multiple hash iterations with salt. Unlike DFT, DWT decomposes the audio into time-frequency subbands, allowing for embedding in regions less perceptible to human hearing. This not only improves the robustness of watermarking but also retains high audio quality. Watermarking is done frame-wise: each audio segment is compressed and its metadata is embedded in the encrypted audio. During decryption, authorized users validate the signal's integrity using embedded metadata. If intact, the audio is decrypted directly. If tampered, the compressed metadata allows approximate recovery of the original audio.

V. Methodology

The overall system architecture comprises six core modules:

1. Key Generation Module:
   - Uses PBKDF2HMAC with SHA-256 and salt to derive a strong symmetric key from a user password.

2. Encryption Module:
   - Applies scrambling and multiplication to audio signal.
   - Performs AES-GCM encryption to provide confidentiality and integrity.
   - Applies Fernet encryption as an additional layer.

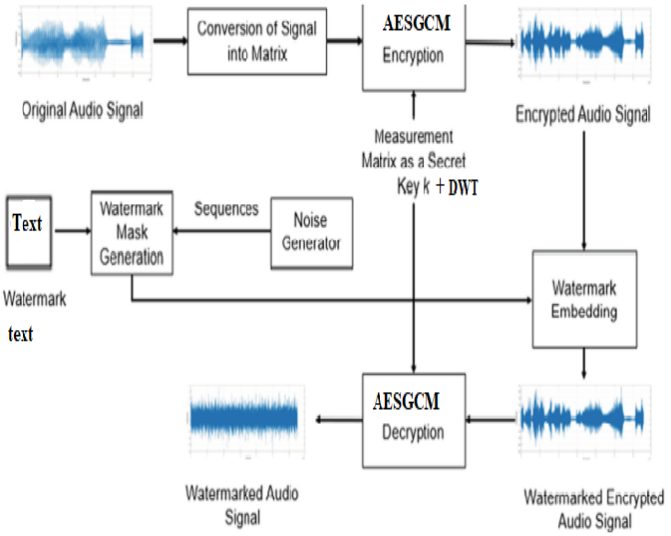
3. Compression and Framing:
   - Splits audio into fixed-size frames.
   - Compresses frames to reduce storage and enhance resilience.

4. Watermark Embedding:
   - Embeds compressed frames into the encrypted signal using DWT.
   - Each embedded watermark includes frame number and compressed data.

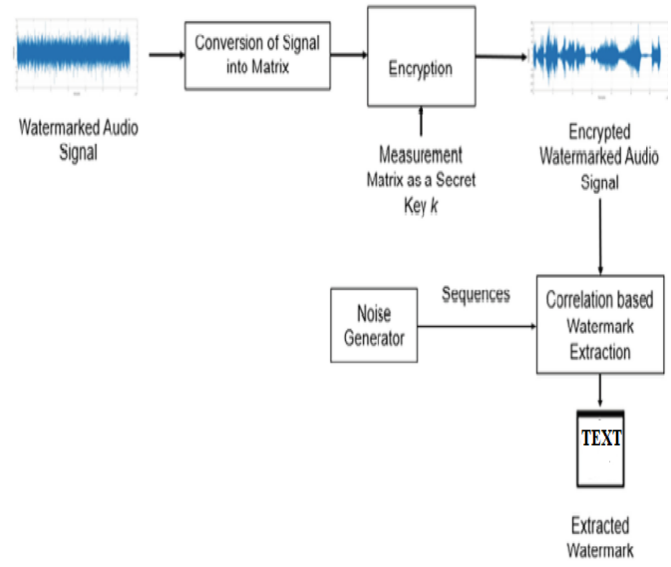
5. Integrity Verification and Decryption:
   - Validates data using authentication tag from AES-GCM.
   - If signal is authentic, decrypts using Fernet.

6. **Attack Detection and Audio Recovery**:
   - If watermark indicates tampering, identifies and reconstructs affected frames using embedded data.

VI. System Architecture



(a)



VII. Results and Discussion

Experimental evaluation was conducted using a set of real-world audio signals subjected to various distortions including Gaussian noise, MP3 compression, and time-scaling attacks.

The performance was assessed based on:
- Bit Error Rate (BER) of watermark recovery.
- Signal-to-Noise Ratio (SNR) of reconstructed audio.
- Detection accuracy for tampered frames.

Results showed that the proposed system:
- Maintains an average SNR of above 35 dB post-decryption.
- Recovers watermarks with over 98% accuracy even under MP3compression.
- Detects tampered segments with over 95% precision.

Compared to DFT-based approaches, the proposed DWT-enhanced system exhibited greater resilience, faster decryption times (due to Fernet), and support for secure recovery.

Conclusion

This paper presents a forward-thinking solution to the problem of secure audio storage and transmission. By integrating AES-GCM, Fernet, PBKDF2HMAC, and DWT into a unified architecture, the system achieves quantum-safe encryption, robust watermarking, and approximate reconstruction. Future work includes extending this scheme to real-time streaming environments and integrating machine learning for adaptive watermarking based on audio context.

REFERENCES

[1] 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.
[2] J. He et al., “A novel audio watermarking algorithm robust against recapturing attacks,” *Multimedia Tools Appl.*, vol. 82, no. 12, pp. 18599–18616, May 2023.
[3] Z. Su et al., “Window switching strategy based semi-fragile watermarking for MP3 tamper detection,” *Multimedia Tools Appl.*, vol. 76, no. 7, pp. 9363–9386, Apr. 2017.
[4] C.-J. Chen et al., “Digital audio watermarking using optimized DWT low-frequency coefficients,” *Multimedia Tools Appl.*, vol. 80, no. 2, pp. 2413–2439, Jan. 2021.