International Journal of Digital Crime and Forensics
Volume 16 • Issue 1

A Novel Watermarking Scheme for Audio Data Stored in Third Party Servers

Fuhai Jia, Xinyang University, China
Yanru Jia, Xinyang University, China
Jing Li, Xinyang University, China
Zhenghui Liu, Xinyang Normal University, China*

ABSTRACT

To improve the security and privacy of audio data stored in third party servers, a novel watermarking scheme is proposed. Firstly, the authors split the host signal into frames and scramble each frame to get the encrypted signal. Secondly, they generate watermark bits by using the frame number and embed them into each frame of the encrypted signal, which is the data that will be uploaded to the third party servers. For the users, they can download the encrypted data and verify the data is intact or not. If the data is intact, the users decrypt the data to get the audio signal. If the audio signal is attacked in the process of transmission, they can also locate the location of the attacked frame. The experimental results show that the method proposed is effective not only for encrypted signals, but also for the encrypted signals after decryption.

KEYWORDS

Content Security, Digital Audio, Digital Forensics, Watermarking

INTRODUCTION

The development of digital signal processing technology facilitated communication among individuals. However, this progress has also increased concerns regarding the potential leakage of users' private data. For example, the popularity of recording devices has empowered individuals to create their own audio signals. Yet, managing a large volume of audio signals poses a problem to consider for the owners of the signals in terms of storage. In pursuit of convenience, some upload their works to third-party storage centers. However, entrusting their data to external storage centers exposes their works to potential threats, as these centers operate outside of their control (Kuang et al., 2020; Razali et al., 2021). To improve the security of the data stored in third-party centers, a watermarking algorithm is proposed in this article.

The field of digital watermarking technology has seen more than 10 years of research, with many studies exploring its application and methods (Hua et al., 2016). Generally speaking, digital watermarking schemes use the redundancy in audio signals and auditory insensitivity of human ears to embed watermark bits into the host signal without degrading the quality. These schemes can be categorized based on their different purposes.

DOI: 10.4018/IJDCF.340382 *Corresponding Author

One category, called robust digital watermarking, is used in copyright protection (Chen et al., 2018; Jiang et al., 2019; Kosta et al., 2022; Salah et al., 2021). The other category, called fragile or semi-fragile digital watermarking, is used for forensic purposes (Chen et al., 2010).

In Yong et al. (2014), a robust audio watermarking scheme was proposed, where the authors embedded watermark bits and synchronization codes into the host signal to generate the watermarked signal. During decoding, users could determine whether the signal had been scaled by observing changes in the synchronization code's position. If scaling was detected, users could calculate the scale factor, allowing them to reduce the impact of attacks and improve the scheme's robustness.

Liu et al. (2021) proposed an audio watermarking algorithm for tracing the re-recorded audio sources. In their work, the authors introduced the LMC feature and conducted an analysis of its characteristics. Then, the authors embedded watermark bits by quantizing discrete cosine transform (DCT) intermediate frequency coefficients to quantize LMC features. The LMC feature has robustness against re-recording attacks, enabling the scheme to accurately extract correct watermark bits from the attacked signals.

In Liu et al. (2022), an audio watermarking scheme for encrypted audio was introduced, addressing a relatively unexplored are in audio watermarking. The authors cut the host signal into frames and then scrambled each frame to generate encrypted audio. Then, they embedded the frame number by quantifying the signal energy ratio into the encrypted frame. This approach enables the scheme to identify the tampered location in the attacked signal, allowing for the substitution of attacked frames with 0 amplitude samples to reconstruct the signal.

However, a limitation of the scheme proposed in Liu et al. (2022) is that if downloaded data is intact, users can decrypt the audio signal, placing it in an unprotected range. Consequently, if the decrypted signal is attacked during the transmission, the scheme lacks the ability to verify its integrity.

To solve the above problems and improve the security of the encrypted audio signals, this article proposes a novel watermarking scheme. Initially, the host signal is encrypted, followed by the embedding of watermark bits into the encrypted signal. The process begins with segmenting the host signal into frames, each of which is then scrambled to produce the encrypted signal. Then, binary bits representing the frame numbers are embedded into the frames of the encrypted signal to generate the watermarked data, which is uploaded to third-party servers.

If users download the watermarked data, they can divide the data into frames and verify their integrity. Intact frames can then be decrypted to retrieve the original audio signal, enabling direct comprehension by users. Besides, if the decrypted signal is attacked, the scheme can verify the authentication of the attacked signal and locate the compromised frames. The main contributions of this article are described as follows:

- The study presents the encryption and decryption methods of audio signals, and defines the feature of encrypted audio signal. Then, the study designs the watermark embedding method by quantifying the feature.
- The study proposes a novel watermarking scheme based on the defined feature. The scheme not only protects large audio signals stored on third-party servers but also verifies downloaded data integrity. Furthermore, the scheme provides an authentication method for audio signals post-decryption.

The article is organized as follows. The next section introduces the encryption method for host signal. Then, the study describes the proposed scheme, watermark generation, and methods for embedding and extraction. The scheme's performance is then reviewed before the study's conclusion is summarized.