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.

ENCRYPTION

Denote A as the L length speech signal, $A=\left\{a_l,1\le l\le L\right\}$, where a_l is the l-th sample. Based on the logistic chaotic map in equation (1), the L length pseudo-random sequence is obtained, denoted by $Y=\left\{y_l\left|l=1,2,\cdots,L\right.\right\}$. In equation (1), k is the initial value, serving as the key of the watermarking system, $3.5699\le\mu\le 4$ (Liu et al., 2022). Signal A is encrypted using the following steps:

$$y_{l+1}=\mu y_l(1-y_l),y_0=k \tag{1}$$

1. Signal A is cut into P frames. The i-th frame is denoted by $A_i=\left\{a_{i,t}\left|t=1,2,\cdots,L/P\right.\right\}$.
2. The first L/P length sequence of Y is selected, denoted by $Y_1=\left\{y_t\left|t=1,2,\cdots,L/P\right.\right\}$. Then, the elements in Y_1 is assorted in ascending order based on equation (2), where $h\left(t\right)$ is the address index of the sorted chaotic sequence.

$$y_{h(t)}=\text{ascend}\left(y_t\right),t=1,2,\cdots L/P \tag{2}$$

3. Each frame A_i is scrambled as $1\le p\le P$, denoting the scrambled signal as B_i. $B_i=\left\{b_{i,t}\left|t=1,2,\cdots,L/P\right.\right\}$ is denoted, where $b_{i,t}$ is the t-th sample after being scrambled (see equation (3)). If B is denoted as the encrypted signal, then $B=\left\{B_1\cup B_2\cup\cdots\cup B_P\right\}$.

$$b_{i,t}=a_{i,h(t)},\ t=1,2,\cdots L/P \tag{3}$$

THE SCHEME

To protect the audio signals stored on third-party servers, the study proposes a watermarking scheme. This scheme serves a dual purpose: it protects lager audio signals stored on these servers and verifies the integrity of data downloaded from them. At the same time, the scheme provides authentication for audio signals after decryption.

To effectively detect and locate attacked signals, the frame number is encrypted into the encrypted data. Then, the frame number is extracted from the attacked content.

Watermark Generation

Based on the previous section, the audio signal is encrypted as $B=\left\{B_1\cup B_2\cup\cdots\cup B_P\right\}$, in which B_i is the i-th frame of the encrypted signal. The frame number of B_i is i. The frame number i is converted into M length binary bits, denoted by $W_i=\left\{w_{i,1},w_{i,2},\cdots,w_{i,M}\right\}$. If the length is less than M, 0 is added to satisfy the length requirement. For the first frame B_1, the frame number is 1. It is converted to 0000000001 (set M = 10 in this article). Thus, $W_1=\left\{0,0,0,0,0,0,0,0,0,1\right\}$.

Watermark Embedding

$B=\left\{B_1\cup B_2\cup\cdots\cup B_P\right\}$ is obtained based on the encrypted signal. The following takes the embedding of W_1 into the first frame B_1 as an example to introduce the embedding method.

1. We cut B_1 into 2*M* segments and denote the *m*-th segment as $B_{1,m}$, $1 \le m \le 2M$. The length of $B_{1,m}$ is $L/2MP$, $B_{1,m} = \left\{b_{1,m}^1, b_{1,m}^2, \cdots, b_{1,m}^{L/2MP}\right\}$.
2. The security feature (SF) of $B_{1,m}$ is calculated using equation (4).

$$F_{1,m} = \sum_{t=1}^{L/2MP} \log_2 \frac{b_{1,m}^t}{y_t},\ 1 \le t \le L/2MP,\ 1 \le m \le 2M \tag{4}$$

3. In this study, the first frame embeds W_1 into the first *M* segments $B_{1,m}$, $1 \le m \le M$. Then, W_1 is embedded into the rest of the *M* segments $B_{1,m}$ similarly, $M+1 \le m \le 2M$. Using the following method, $w_{1,m} \in W_1 = \left\{w_{1,1}, w_{1,2}, \cdots, w_{1,M}\right\}$ is embedded into $B_{1,m}$. If $w_{1,m} = 0$, equation (5) is used to quantify the SF of $B_{1,m}$. If $w_{1,m} = 1$, equation (6) is used to quantify the SF of $B_{1,m}$.

$$QF_{1,m} = \begin{cases} \left\lfloor F_{1,m}/\Delta \right\rfloor \times \Delta + \Delta/2, & EF_{1,m} = 0 \\ \left(\left\lfloor F_{1,m}/\Delta \right\rfloor - 1\right) \times \Delta + \Delta/2, & EF_{1,m} = 1 \end{cases} \tag{5}$$

$$QF_{1,m} = \begin{cases} \left\lfloor F_{1,m}/\Delta \right\rfloor \times \Delta + \Delta/2, & EF_{1,m} = 1 \\ \left(\left\lfloor F_{1,m}/\Delta \right\rfloor + 1\right) \times \Delta + \Delta/2, & EF_{1,m} = 0 \end{cases} \tag{6}$$

where $QF_{1,m}$ is the SF after being quantified and $EF_{1,m} = \left\lfloor F_{1,m}/\Delta \right\rfloor \bmod 2$ and Δ is the quantification step.

4. If the watermarked signal is denoted as $WB_{1,m}$ and $WB_{1,m} = \left\{wb_{1,m}^1, wb_{1,m}^2, \cdots, wb_{1,m}^{L/2MP}\right\}$, $wb_{1,m}^t$ can be calculated by equation (7).

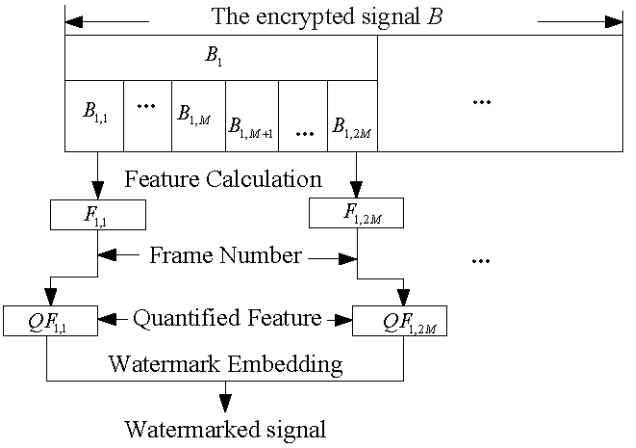
$$wb_{1,m}^t = b_{1,m}^t \times 2^{QF_{1,m} - F_{1,m}},\ 1 \le t \le L/2MP \tag{7}$$

5. The segmentation and embedding methods of the other frames are similar to the first frame. By using the same method, the watermark W_i, $1 \le i \le P$ is embedded into the encrypted signal B. The process of segmentation and embedding is shown in Figure 1.

Watermark Extraction and Forensics

This section will verify data in two cases. Case 1 will verify the integrity of the encrypted data downloaded from third-party servers. If the encrypted data is intact, the data is decrypted to get the audio signal, which may have been attacked in the process of transmission. Case 2 will authenticate the audio signal obtained after decryption.

Figure 1. Segmentation and Watermark Embedding



Case 1: Verification of Encrypted Data

It is assumed that the encrypted data downloaded by the user is *D*, $D = \left\{d_l, 1 \le l \le L'\right\}$, where L' is the length of the downloaded data. It may be different to the length of the original L.

1. The L' length data *D* is cut into frames. The length of each frame is L/P. Then, the data *D* can be represented by $D = \left\{D_1 \cup D_2 \cup \cdots \cup D_{P'}\right\}$, where D_i represents the *i*-th frame, $1 \le i \le P$.
2. The first frame D_1 is selected and divided into 2*M* segments. The *m*-th segment is denoted $D_{1,m}$, $1 \le m \le 2M$. The length of $D_{1,m}$ is $L/2MP$, $D_{1,m} = \left\{d_{1,m}^1, d_{1,m}^2, \cdots, d_{1,m}^{L/2MP}\right\}$, where $d_{1,m}^t$ is the *t*-th sample of $D_{1,m}$.
3. Based on equation (4), the SF of $d_{1,m}^t$, $1 \le t \le L/2MP$ is calculated, denoted by $F_{1,m}'$.
4. Using equation (8), the watermark bit $w_{1,m}^t$ is extracted from the *m*-th segment $D_{1,m}$, $1 \le m \le 2M$. The 2M length bits extracted are denoted by $W_1' = \left\{w_{1,1}', w_{1,2}', \cdots, w_{1,2M}'\right\}$.

$$w_{1,m}^t = F_{1,m}' \bmod 2 \tag{8}$$

5. For the watermark bits belonging to W_1', the frame D_1 is intact if the first *M* bits are similar to the last *M* bits. Otherwise, it indicates that the frame D_1 is attacked. If the frame is intact, the extracted watermark bits satisfy equation (9).

$$\sum_{m=1}^{M} w_{1,m}' \oplus w_{1,M+m}' = 0 \tag{9}$$

6. Using this method can authenticate all the intact frames. Suppose that the *i*-1-th frame is intact and the *i*-th frame is attacked. Then, move and authenticate the next *L*/*P* samples until we find that the *L*/*P* continuous samples can go through the authentication process successfully. The *L*/*P* continuous samples are denoted by $D_{i'}$. The content between the *i*-1-th and the i'-th frame is the attacked signal.

Case 2: Verification of Audio Signal

Supposing that the encrypted data D is intact, we decrypt signal D to get the audio signal. The following gives the forensics method for the audio signal.

1. The data D is cut into P frames. The i-th frame is denoted by $D_i = \left\{ d_{i,t} \middle| t = 1,2,\cdots, L/P \right\}$, $1 \le i \le P$.
2. Based on the scrambling method, anti-scrambling operation is performed on each frame D_i, $1 \le i \le P$. The obtained signal is decrypted, denoted by $G_i = \left\{ g_{i,t} \middle| t = 1,2,\cdots, L/P \right\}$.
3. All the frames are combined to get a complete decrypted signal $G = \left\{ G_1 \bigcup G_2 \bigcup \cdots \bigcup G_P \right\}$. The decrypted signal may be attacked during transmission. In this section, we suppose that $G_1 = \left\{ g_{1,t} \middle| t = 1,2,\cdots, L/P \right\}$ is the first frame. In the following, we give the authentication steps by using the method proposed in this article.
   i. We use a segmentation method similar to the Case 1, dividing G_1 into $2M$ segments. We denote the m-th segment as $G_{1,m}$, $1 \le m \le 2M$.
   ii. We calculate the feature of $G_{1,m}$ by using equation (10).

$$FG_{1,m} = \sum_{t=1}^{L/2MP} \log_2 g_{1,m}^t - \log_2 y_t \tag{10}$$

   where $g_{1,m}^t \in G_{1,m}$, $G_{1,m} = \left\{ g_{1,m}^1, g_{1,m}^2, \cdots, g_{1,m}^{L/2MP} \right\}$.

   iii. Using equation (11), we extract the watermark bit $gw_{1,m}$ based on the feature $FG_{1,m}$.

$$gw_{1,m} = FG_{1,m} \bmod 2,\ 1 \le m \le 2M \tag{11}$$

   iv. Then, we obtain all the watermark bits $GW_1 = \left\{ gw_{1,1}, gw_{1,2}, \cdots, gw_{1,2M} \right\}$, as extracted from the first frame G_1.
   v. Based on the watermark bits extracted from G_1, and using the method similar to steps 5 and 6 in Case 1, we can verify the authenticity of the frame G_1. If $\sum_{m=1}^{M} gw_{1,m} \oplus gw_{1,M+m} = 0$, the G_1 frame is intact. Otherwise, it indicates that the frame has been attacked.

Repeating the above steps can verify all the frames of the audio signal G. The process of the verification of encrypted data and audio signal is shown in Figure 2.

Therefore, by combining with the embedding method, for audio signals that need to be stored in a third-party storage center, we can first adopt the encryption and watermarking methods outlined in this article to generate encrypted and watermarked data. Then, we upload these data to a third-party storage center. When necessary, we download the data and verify the authenticity of the downloaded data. After judgment, for the real data, we decrypt it to get the audio signal. If the audio signal is attacked, users can locate the attacked frame. The implementation method is shown in Figure 3.

Figure 2. Verification of Encrypted Data and Audio Signal

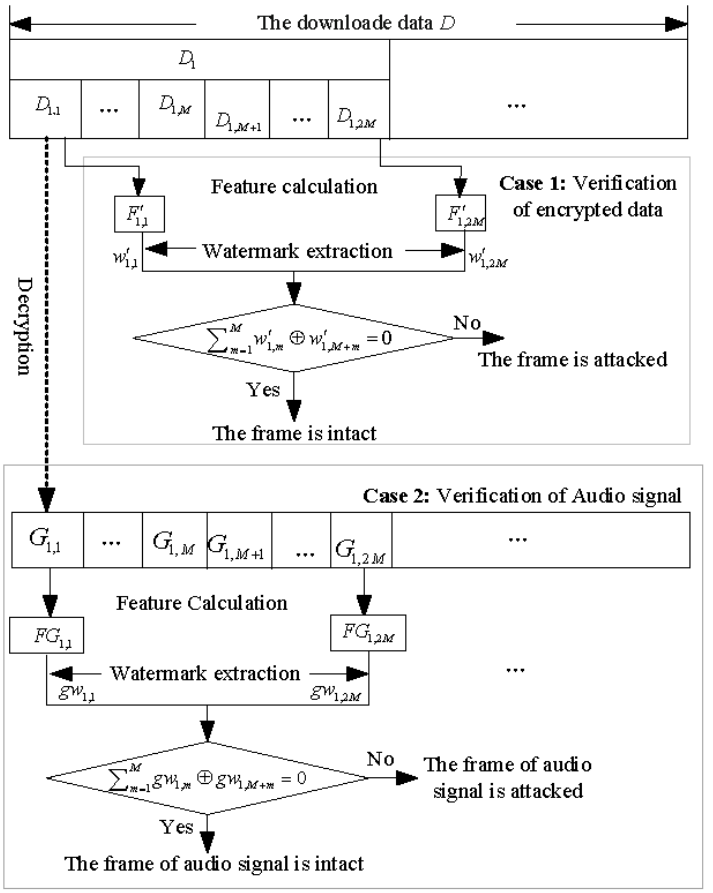
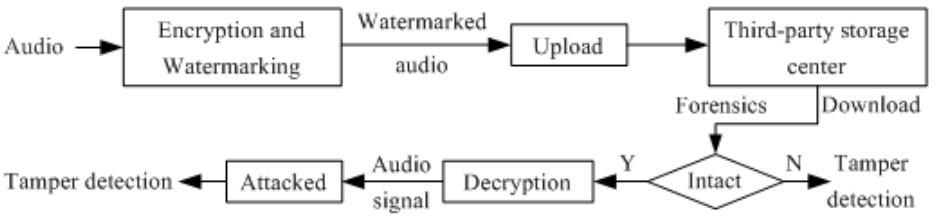


Figure 3. Implementation Method of the Proposed Scheme



ANALYSIS OF PERFORMANCE

This section tests the inaudibility of watermark embedding, confirming that it does not reduce the auditory quality of the audio signal. Besides, the innovation of the scheme proposed in this article focuses on two aspects:

1. The scheme's capability to verify the authenticity of encrypted signals.
2. The scheme's ability to detect tampering in encrypted signals after decryption.

Therefore, in this section, the authors' main objective is to test the tamper detection capabilities of both the encrypted signal and the signal after decryption. The experimental parameters used in this study are $L = 441{,}000$, $P = 10$, $M = 10$, $k = 0.287$, and $\mu = 3.958$.

Inaudibility

A total of 550 audio signal segments are selected from the library. Based on the scheme, each audio is encrypted and the watermark bits are embedded into all the signals. The signal-to-noise ratio (SNR) is used to test the inaudibility of the watermark embedding, as defined in equation (12).

$$\mathrm{SNR} = 10\lg\left(\frac{\sum_{l=1}^{L} a_l^{\,2}}{\sum_{l=1}^{L}\left(a_l - g_l\right)^2}\right) \tag{12}$$

where a_l and g_l are the l-th original and watermarked signal. When the SNR value is greater than 20, the watermark bit embedded into audio is inaudible (Liu et al., 2021).

Table 1 shows the maximum (Max), average (Aver), and minimum (Min) values of SNR after the SNR calculation of the watermarked signal. Meanwhile, the inaudibility of some latest schemes are tested, while the inaudibility of the algorithm is compared with the schemes. The embedding capacity of all the schemes is 20bps. The comparison results are shown in Table 1.

Based on the results shown in Table 1, it can be seen that the SNR value is greater than the schemes (Chen et al., 2018; Hu et al., 2022; Jiang et al., 2019; Liu et al., 2022). This indicates that the watermarked signals have better auditory quality in this article.

Audio Encryption

This section selects one signal from the library. According to the algorithm, the study encrypts the signal and verifies the encrypted data and decrypted signal, respectively. The signal selected is shown in Figure 4, which includes 410,000 samples.

1. The signal shown in Figure 4 is cut into P frames. Based on the logistic map and the parameters $k = 0.287$, $\mu = 3.958$, the pseudo-random sequence $Y_1 = \left\{y_1, \cdots, y_{44100}\right\} = \left\{0.2870, \cdots, 0.2751\right\}$ is achieved. The scrambling method produces the encrypted signal as shown in Figure 5.

Table 1. SNR Values of Different Schemes

Schemes	SNR		
	Max	Aver	Min
Ref. (Chen, Wang, & Tian, 2018)	22.3	20.1	18.5
Ref. (Jiang, Huang, & Quan, 2019)	22.6	21.4	19.2
Ref. (Liu, Cao, & Lin, 2022)	24.7	22.6	20.9
Ref. (Hu, Lu, & Ma, 2022)	23.1	21.5	19.7
Our	31.3	26.4	22.8

Figure 4. Selected Signal

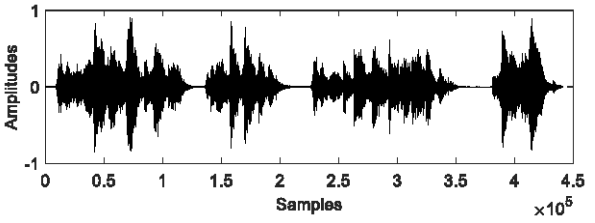
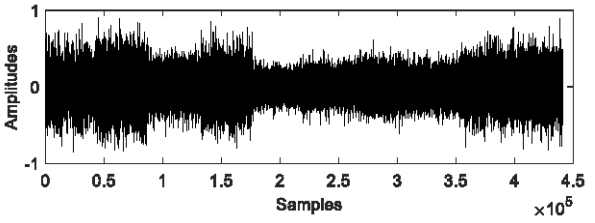


Figure 5. Encrypted Signal



2. The first frame is divided into $M(M = 20)$ segments and the SF of each segment is calculated. Based on the watermark generation and embedding method, the watermark $W_1 = \{0,0,0,0,0,0,0,0,0,1\}$ is embedded into two consecutive 10 segments (the first 10 and second 10 segments). Similarly, the other watermark W_2, W_3, …, W_{10} is embedded into the remaining nine frames to obtain the watermarked data. The encrypted data can then be uploaded to a third-party storage center. Figure 6 shows the watermarked data.

Encrypted Data Authentication

The study assumes that some samples of the data downloaded by the user from the storage center have been deleted, as shown in Figure 7. The attacked signal is verified in the following:

1. For the downloaded signal, the first 44,100 samples are one frame. According to the watermark extraction method, the frame is divided into 20 segments before the watermark bits are extracted $W_1' = \{0,0,0,0,0,0,0,0,0,1,\ \ 0,0,0,0,0,0,0,0,0,1\}$. Based on the verification method, the frame is intact and the frame is the first frame.

Figure 6. Watermarked Data

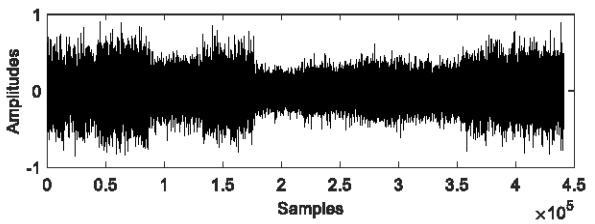
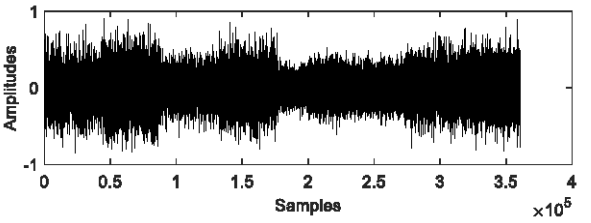


Figure 7. Attacked Signal Downloaded From the Storage Center



2. Repeat the above step, searching for the intact frames. The frame number of the intact frame is shown in Figure 8, which indicates that the signals of the frame with TM = 1 are intact.

The results shown in Figure 8 illustrate that the fifth through seventh frames have been attacked.

Encrypted Signal Authentication

If the downloaded data is intact, users will decrypt the data to obtain the decrypted signal (see Figure 8). Figure 9 illustrates the decrypted signal compromised by another attacker.

Similarly, the study takes the first 44,100 samples as one frame, splitting the frame into 20 segments. Then, the sequence Y_1 is used and equation (10) calculates the features of the 20 segments. According to the calculated features, the watermark bits are extracted and authenticated regardless of the frame's condition. The number of the intact frame is shown in Figure 10, with the result indicating that, for the signal in Figure 9, the eighth and ninth frames are attacked.

This study provides a comprehensive analysis of proposed schemes by Hu et al. (2022), Kosta et al. (2022), Liu et al. (2022), and Salah et al. (2021). Table 2 shows the comparison of results, with ES representing the ability to encrypt audio signals, FED representing the ability of forensics on encrypted data, and DFAS representing the ability of forensics on audio signals after decryption.

Figure 8. Intact Signal Decrypted

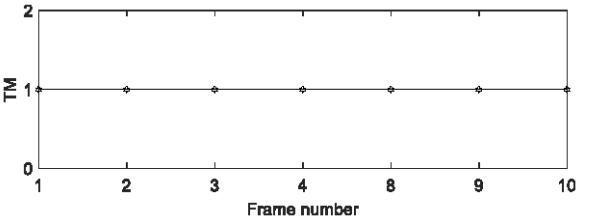


Figure 9. Attack Signal as Shown in Figure 6

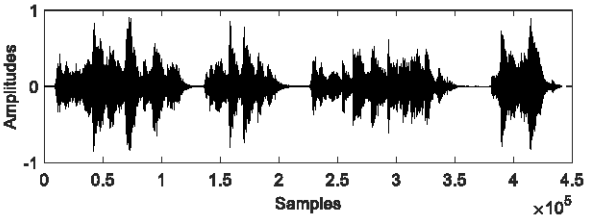


Figure 10. Frame Number of the Intact Frame for the Signal Shown in Figure 9

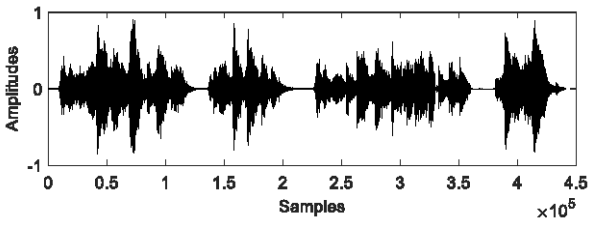


Table 2. Security and Forensics Capabilities of Different Schemes

Schemes	ES	FED	DFAS
Ref. (Kosta et al., 2022)	No	No	No
Ref. (Salah et al., 2021)	No	No	No
Ref. (Liu et al., 2022)	Yes	Yes	No
Ref. (Hu et al., 2022)	No	No	NO
Our	Yes	Yes	Yes

By studying the schemes proposed in Hu et al. (2002), Kosta et al. (2022), Liu et al. (2022), and Salah et al. (2021), the authors concluded that the scheme not only protects the lager audio signals through the encryption method but also verifies whether the encrypted data is intact. Besides, the scheme provides the authentication method for the audio signals after decryption.

Theoretical Basis

The following provides a theoretical analysis. For the encrypted signal, the authors utilize the $F_{1,m}$ feature before extracting the watermark bit by $w_{1,m} = F_{1,m} \bmod 2$. Similarly, for the encrypted signal after decryption, users need to use the $F_{1,m}$ feature to extract the same watermark information.

According to equation (4), the $F_{1,m}$ feature is the sum of each sample divided by the corresponding Y_1 element. By logarithm properties, it appears that:

$$F_{1,m} = \sum_{t=1}^{L/2MP} \log_2 b_{1,m}^t - \log_2 y_t \tag{13}$$

For the signal after decryption, the feature (denoted by $FG_{1,m}$) can be calculated with equation (14):

$$FG_{1,m} = \sum_{t=1}^{L/2MP} \log_2 g_{1,m}^t - \log_2 y_t \tag{14}$$

The samples $g_{1,m}^t$, $1 \le t \le L/2MP$ can be obtained by the samples $b_{1,m}^t$, $1 \le t \le L/2MP$ after anti-scrambling. Thus, for the $L/2MP$ samples, $FG_{1,m} = F_{1,m}$. Additionally, the users can extract the same watermark bits from the decrypted signal.

CONCLUSION

To enhance the security of audio signals stored in a third-party storage center, this article proposes a double watermarking scheme. The scheme not only verifies the integrity of the encrypted signal but also proves effective for the decrypted version. First, the authors cut the host signal into frames and scramble each frame to get the encrypted signal. Then, the authors use frame numbers to generate watermark bits, embedding them into the encrypted signal. This obtains the data uploaded to third-party servers. When needed, users can download and authenticate the encrypted data. If the encrypted data is intact, users can decrypt it to get the decrypted signal. If the decrypted signal is compromised during transmission, the scheme can identify tamper locations. Experimental results prove the effectiveness of the proposed scheme.

In this article, signal encryption mainly uses the scrambling method. Although this approach offers high efficiency, the security of the proposed algorithm could be improved compared with more complex encryption algorithms. In future work, the authors will focus on improving the security of encrypted signals without degrading other performance metrics.

REFERENCES

Chen, L. I., Wang, K., & Tian, L. (2018). Audio watermarking algorithm in MP3 compressed domain based on low frequency energy ratio of channels. *Jisuanji Yingyong*, *38*(8), 2301–2305.

Chen, N., Zhu, M. Y., & Liu, S. (2010). A new fragile audio watermarking scheme. *International Conference on Audio Language and Image Processing,* 367–372.

Hu, X. Y., Lu, W., Ma, M., Sun, Q., & Wei, J. (2022). A semi fragile watermarking algorithm based on compressed sensing applied for audio tampering detection and recovery. *Multimedia Tools and Applications*, *81*(13), 17729–17746. doi:10.1007/s11042-022-12719-0

Hua, G., Huang, J. W., Shi, Y. Q., Goh, J., & Thing, V. L. L. (2016). Twenty years of digital audio watermarking: A comprehensive review. *Signal Processing*, *128*(11), 222–242. doi:10.1016/j.sigpro.2016.04.005

Jiang, W., Huang, X., & Quan, Y. (2019). Audio watermarking algorithm against synchronization attacks using global characteristics and adaptive frame division. *Signal Processing*, *162*, 153–160. doi:10.1016/j.sigpro.2019.04.017

Kosta, P., Slavko, K., Igor, D., & Adam, W. (2022). Robust speech watermarking by a jointly trained embedder and detector using a DNN. *Digital Signal Processing*, *122*, 103381. doi:10.1016/j.dsp.2021.103381

Kuang, Y. J., Li, Y., & Li, P. (2020). A searchable ciphertext retrieval method based on counting bloom filter over cloud encrypted data. *IAENG International Journal of Computer Science*, *47*(2), 271–277.

Liu, Z. H., Cao, Y., & Lin, K. J. (2022). A watermark scheme for encrypted audio signal. *IAENG International Journal of Applied Mathematics*, *52*, 3–22.

Liu, Z. H., Zhao, X. L., & Jin, Y. (2021). Audio watermarking algorithm for tracing the re-recorded audio source. *IAENG International Journal of Computer Science*, *48*, 4–35.

Razali, N. A. M., Muhamad, W. N. W., & Ishak, K. K. (2021). Secure blockchain-based data-sharing model and adoption among intelligence communities. *IAENG International Journal of Computer Science*, *48*(1), 18–31.

Salah, E., Amine, K., Redouane, K., & Fares, K. (2021). A fourier transform based audio watermarking algorithm. *Applied Acoustics*, *172*, 107652. doi:10.1016/j.apacoust.2020.107652

Yong, I., Natgunanathan, G., & Song, W. (2014). Patchwork-based audio watermarking method robust to de-synchronization attacks. *IEEE/ACM Transactions on Audio, Speech, and Language Processing*, *22*(9), 1413–1423. doi:10.1109/TASLP.2014.2328175

Zhenghui Liu was born in 1983. He received the B.S. degree from Luoyang Normal University, Luoyang, in 2005; M.S. degree from Xinyang Normal University, Xinyang, in 2010, and Ph.D. degrees from the School of Information Science and Technology, Southwest Jialtong University, Chengdu, in2014. He currently works as the post doctor with the College of Information Engineering, Shenzhen University, Shenzhen, China. His current research interests include multimedia information security and audio content authentication.