A Watermark Scheme for Encrypted Audio Signal

Zhenghui Liu, Yi Cao, Kejia Lin

Abstract—**In order to protect the privacy of audio signals stored on third-party servers, a watermarking scheme for encrypted audio is proposed. We define an audio feature signal energy ratio and propose an audio encryption method, containing scrambling and sample value mapping. We use frame number to generate watermark and give the embedding method by quantifying signal energy ratio feature. Experimental results show that, for watermarked audio being attacked, the scheme can locate the attacked frame. Based on the location results, we use 0 amplitude samples to substitute the attacked frames and decrypt the audio signal. The 0 amplitude signals can be dispersed to different parts after anti-scrambling and do not influence the expressed meaning of original signal. In this sense, the scheme can recover the meaning of the attacked audio to some extent.**

Index Terms—**Digital watermark, encrypted audio, content authentication, tamper recovery**

I. Introduction

The popularity of high-speed network provides convenience for people to store audio data on third-party storage centers. However, for data owners, the third-party servers are not within their trusted domains, and their sensitive data face serious security threats[1]. Generally, audio data involves sensitive information such as personal or business secret, and they are usually encrypted before uploading. If the audio data stored in the third party is modified by the attacker, the audio data downloaded by the user will not get the desired information. The data loss incidents of third-party servers appear from time to time [2], [3].

In recent years, many image encryption algorithms based on chaotic systems have emerged [4]-[7]. Reference [4] proposed a chaos-based image encryption system by introducing the diffusion effect in the permutation phase to reduce the overall encryption time. In order to enhance the complexity of the system and the size of the key space, multiple chaotic systems were chosen to be superimposed to increase the difficulty of breaking the encryption system[5]-[7].

There are relatively few audio encryption schemes based on chaotic systems [8], [9]. Reference [8] introduced a three dimensional chaotic systems. Then a lossless audio encryption scheme was introduced utilizing the proposed chaotic maps. Reference [9] proposed an audio encryption scheme based on a substitution-permutation algorithm using DNA encoding. Experimental results demonstrated that the scheme can resist the chosen cipher text and chosen-plaintext attacks.

It is true that chaotic system plays an important role in image and audio encryption. However, the chaotic system is different from cryptography. The reason is that, the phase space of chaotic system is in a continuous real number domain and cryptography is usually defined over a finite discrete domain. These may produce dynamical performance degradation during digital implementation due to the finite accuracy of computers [10], [11].

In order to improve the security of encrypted audio signal based on chaotic system, we encrypt the audio signal based on a chaotic system firstly. Then we embed watermark into the encrypted signal before uploading. For the signals in third-party storage centers being attacked, the method can locate the attacked segment and recovery the attacked signals. We define the energy ratio feature of audio signal and analyze the properties of the feature. A pseudo-random sequence is divided into different sets, and each set is mapped onto the corresponding frame number. The set and frame number are all regarded as watermark and embedded. The set as the identification of each frame is used to locate the watermarked and attacked segments precisely. Theoretical analysis and experimental results demonstrate that, the encryption method can provide a certain degree of security for speech signal. The watermarked audio is inaudible, and the embedding method has the ability of identifying tamper location precisely and a good tamper recovery capacity.

The organization of this paper is as follows. Section II introduces the signal energy ratio, including the definition and properties. Section III describes the scheme proposed. Section IV analyzes the performance of the algorithm theoretically, security and tamper location ability. Finally, we summarize the conclusion in section V.

Manuscript received January 28, 2022; revised June 16, 2022.

This work was supported by the Nanhu Scholars Program for Young Scholars of XYNU (Xinyang Normal University), and the Opening Project of Guangdong Provincial Key Laboratory of Information Security Technology.

Z. Liu is an associate professor of School of Computer and Information Technology, Xinyang Normal University, Xinyang 464000, China, Guangdong Provincial Key Laboratory of Information Security Technology, also of Guangdong Key Laboratory of Intelligent Information Processing and Shenzhen Key Laboratory of Media Security, Shenzhen 518060, China, (e-mail: zhenghui.liu@163.com)

Y.Cao is a postgraduate of School of Computer and Information Technology, Xinyang Normal University, Xinyang 464000, China. (e-mail: 230185343@qq.com).

K. Lin is a librarian of Xinyang Normal University Library, Xinyang 464000, China. (e-mail: 190766398@qq.com).

II. Signal Energy Ratio

Watermarking schemes based on public features are vulnerable to substitution attack [12], such as the embedding method based on signal energy [13]. In order to improve the security of watermark embedding, we define the signal energy ratio feature and give a watermark embedding method based on the feature.

A. Signal Energy Ratio Feature

We denote $X=\{x(i),1\le i\le N\}$ and $Y=\{y(i),1\le i\le N\}$ are the two different audio signals, where $x(i)$ and $y(i)$ represent the *i*-th sample of *X* and *Y*. We define the energy ratio of *X* to *Y* by

$$\mathrm{ER}(X,Y)=1000\log 2\left(1+\frac{\sum_{i=1}^{N}x(i)^2}{\sum_{i=1}^{N}y(i)^2}\right) \tag{1}$$

In Eq. (1), $\mathrm{ER}(X,Y)$ represents the energy ratio of *X* to *Y*, $\sum_{i=1}^{N}y(i)^2\ne 0$ and the unit of $\mathrm{ER}(X,Y)$ is dB.

--First, $\mathrm{ER}(X,Y)$ reflects the difference of the energy between *X* and *Y*. The closer $\mathrm{ER}(X,Y)$ is to 1000, the smaller the difference of the energies between *X* and *Y* is. On the contrary, the farther $\mathrm{ER}(X,Y)$ is to 1000, the more the difference of the energies between *X* and *Y* is.

--Second, $\mathrm{ER}(X,Y)\ge 0$, under the condition that the signal *Y* is invariable, a higher value of $\mathrm{ER}(X,Y)$ indicates a larger energy of *X*.

B. Watermark Quantization Method based on Signal Energy Ratio

We denote $E=\mathrm{ER}(X,Y)$, which represents the energy ratio of *X* to *Y*. The audio signal *X* after quantization is recorded as *Q*. $Q=\{q(i),1\le i\le N\}$, where $q(i)$ is the *i*-th sample. Based on Eq. (1), we can get

$$\sum_{i=1}^{N}x(i)^2=\left(2^{\frac{E}{1000}}-1\right)\times\sum_{i=1}^{N}y(i)^2 \tag{2}$$

$$\sum_{i=1}^{N}q(i)^2=\left(2^{\frac{Q_E}{1000}}-1\right)\times\sum_{i=1}^{N}y(i)^2 \tag{3}$$

Combining the Eq. (2) and Eq. (3) we have

$$\frac{\sum_{i=1}^{N}q(i)^2}{\sum_{i=1}^{N}x(i)^2}=\frac{2^{\frac{Q_E}{1000}}-1}{2^{\frac{E}{1000}}-1} \tag{4}$$

Then we can get the relationship between $q(i)$ and $x(i)$, see Eq. (5). Based on Eq. (5), we can obtain samples of the watermarked audio signal according to the quantized features.

$$q(i)=x(i)\times\sqrt{\frac{2^{\frac{Q_E}{1000}}-1}{2^{\frac{E}{1000}}-1}} \tag{5}$$

III. The Scheme

A. Watermark Embedding

We denote *X* as the original signal containing *L* sample points, $X=\{x_l,1\le l\le L\}$.

1) Frame and segmentation: we cut *X* into *N* non-overlapping frames and denote X_i as the *i*-th frame, $X_i=\{x_{i,j},1\le j\le L/N\}$.
2) Pseudo-random sequence generation: we generate two pseudo-random sequences, denoted by $Y^1=\{y_l^1|l=1,2,\cdots,L\}$ and $Y^2=\{y_l^2|l=1,2,\cdots,L/N\}$. The element of Y^1 can be obtained by the logistic chaotic mapping shown in Eq. (6), using the initial value k_1. And the element of Y^2 can be generated in the same way using the initial value k_2.

$$y_{l+1}^1=\mu y_l^1(1-y_l^1),y_0=k_1 \tag{6}$$

where k_1 is the key of the watermarking system. μ is the logistic parameter, $0\le\mu\le 4$. Under the condition that $3.5699\le\mu\le 4$, the sequence generated by Eq. (6) is a pseudo-random distribution state, especially when the value of μ is close to 4. In this paper, $3.5699\le\mu\le 4$.

3) Encryption: we cut Y^1 into *P* non-overlapping frames and denote Y_1^i as the *i*-th frame, $Y_i^1=\{y_{i,j}^1,1\le j\le L/N\}$. Then we encrypt each frame of *X* and denote the encrypted signal as $Z_i=\{z_{i,j},1\le j\le L/N\}$, where $z_{i,j}=x_{i,j}\times y_{i,j}^1$, $1\le i\le N$.
4) Watermark generation: in this paper each frame number is used to generate watermark embedding into the correspond frame. It is worth noting that the frame number *i* not only identifies the audio signal of the *i*-th frame, X_i, but also represents the pseudo-random sequence of the *i*-th segment Y_i, see Eq.(7).

$$X_i=\{x_{i,j},1\le j\le L/N\}\Leftrightarrow i\Leftrightarrow Y_i^1=\{y_{i,j}^1,1\le j\le L/N\} \tag{7}$$

We denote W_i as the watermark being embedded into the *i*-th frame, $W_i=\{w_{i,m}|1\le i\le L/N,1\le m\le M\}$. $w_{i,m}$ can be obtained by the Eq. (8).

$$w_{i,m}=\left\lfloor i/10^{M-m}\right\rfloor\bmod 10 \tag{8}$$

5) Embedding: We take the first frame as an example to introduce the watermark embedding method.
--First, we cut the first frame Z_1 into 2*M* segments. We do a similar operation on Y^2. Then Z_1 can be re-expressed as $Z_1=\{Z_{1,1}\|Z_{1,2}\|\cdots\|Z_{1,M}\|\cdots\|Z_{1,2M}\}$, and Y^2 can be re-expressed as $Y^2=\{Y_1^2\|Y_2^2\|\cdots\|Y_M^2\|\cdots\|Y_{2M}^2\}$.
--Second, we select $Z_{1,1}$, $Z_{1,2}$, $Z_{1,3}$ and Y_1^2, Y_2^2, Y_3^2 to calculate energy ratio, dented by $\mathrm{ER}_{1.1}$, $\mathrm{ER}_{1.2}$, $\mathrm{ER}_{1.3}$, respectively.
--Third, we select the value of $\mathrm{ER}_{1.1}$, $\mathrm{ER}_{1.2}$ and $\mathrm{ER}_{1.3}$

and dente by $V_1 = \lfloor \mathrm{ER}_{1.1} \rfloor \bmod 10$, $V_2 = \lfloor \mathrm{ER}_{1.2} \rfloor \bmod 10$ and $V_3 = \lfloor \mathrm{ER}_{1.3} \rfloor \bmod 10$, using the watermark $w_{1,1}$, $w_{1,2}$ and $w_{1,3}$ to substitute the value of V_1, V_2 and V_3. Then the quantified energy ratio is denoted by $\mathrm{QER}_{1.1}$, $\mathrm{QER}_{1.2}$ and $\mathrm{QER}_{1.3}$. As an example, we assume $\mathrm{ER}_{1.1} = 53.68$, $w_{1,1} = 2$, then we get $V_1 = 3$, and $\mathrm{QER}_{1.1} = 53.68$. Based on the quantified energy ratio $\mathrm{QER}_{1.1}$, we can embed $w_{1,1}$ into $Z_{1,1}$, and get the watermarked signal denoted by $QZ_{1,1}$, using the Eq. (9).

$$qz_{1,j} = z_{1,j} \times \sqrt{\frac{10^{\frac{\mathrm{QER}_{1.1}}{10}} - 1}{10^{\frac{\mathrm{ER}_{1.1}}{10}} - 1}},\ 1 \le j \le L/2MN \tag{9}$$

where $z_{1,j}$ and $qz_{1,j}$ represent the sample of original ($Z_{1,1}$) and watermarked signal ($QZ_{1,1}$). Using the same method we can embed $w_{1,2}$ and $w_{1,3}$ into $Z_{1,2}$, $Z_{1,3}$, and embed $w_{1,1}$, $w_{1,2}$ and $w_{1,3}$ into $Z_{1,4}$, $Z_{1,5}$ and $Z_{1,6}$.

6) Repeating the above steps, we can embed other frame number into other frames. The process of watermark generation and embedding is shown in Fig. 1.

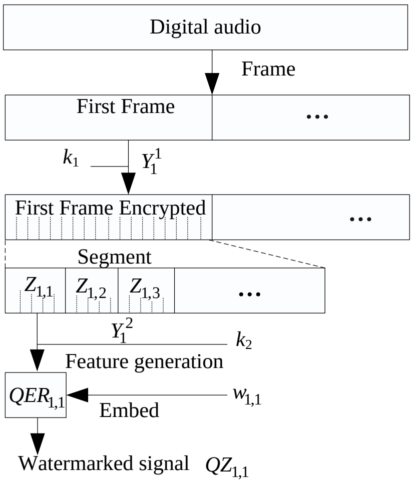

Fig 1. The process of watermark embedding

B. Authentication

Suppose $WZ = \{wz_l, 1 \le l \le WL\}$ as the WL length watermarked signal in encrypted domain, downloaded from third-party servers. In general, we start the forensics from the first frame. We take the first frame as an example to introduce the forensics method.

1) Frame and segmentation: using the method in section III, we cut WZ into L/N length frame and denote the first frame as WZ_1. Then we divide the first frame WZ_1 into $2M$ segments, and we can re-express WZ_1 as $WZ_1 = \{WZ_{1,1} \| WZ_{1,2} \| \cdots \| WZ_{1,M} \| \cdots \| WZ_{1,2M}\}$.

2) Features calculation: we calculate the energy ratio feature of $WZ_1 = \{WZ_{1,1} \| WZ_{1,2} \| \cdots \| WZ_{1,M} \| \cdots \| WZ_{1,2M}\}$ to $Y^2 = \{Y_1^2 \| Y_2^2 \| \cdots \| Y_M^2 \| \cdots \| Y_{2M}^2\}$ for each segment. And we denote the feature as $\mathrm{WER}_{1.1}$, $\mathrm{WER}_{1.2}$, $\cdots$, $\mathrm{WER}_{1.M}$, $\cdots$, $\mathrm{WER}_{1.2M}$, respectively.

3) Watermark extraction and forensics: we extract watermark by the Eq. (10). If $\sum_{m=1}^{M}\left(w_{1,m}^* - w_{1,m+M}^*\right) = 0$, it indicate that the first frame WZ_1 is intact. If $\sum_{m=1}^{M}\left(w_{1,m}^* - w_{1,m+M}^*\right) \ne 0$, it shows that WZ_1 is different from Z_1.

$$w_{1,m}^* = \mathrm{WER}_{1.m} \bmod 10,\ 1 \le m \le M \tag{10}$$

4) Authentication: we suppose $\sum_{m=1}^{M}\left(w_{1,m}^* - w_{1,m+M}^*\right) \ne 0$, and then move sample and forensics next L/N length frame until we find the L/N length frame (denoted by WZ_i), from which watermark extracted satisfies the condition $\sum_{m=1}^{M}\left(w_{i,m}^* - w_{i,m+M}^*\right) = 0$. Then we use $w_{i,m}^*$, $1 \le m \le M$, to reconstruct the frame number i based on the Eq. (11).

$$i = \sum_{m=1}^{M} w_{i,m} \times 10^{M-m} \tag{11}$$

According to the extraction result, we get the conclusion that the signal between the first frame WZ_1 (frame number 1) and the frame WZ_i (frame number i) is different from the original one. So the attacked frame can be obtained by $i-1$. The authentication process is shown in Fig. 2.

5) Decryption: for authenticated audio frames, based on Eq. (7) we can find the segment of pseudo-random sequence corresponding to the frame number. Then we use the Eq. (12) to decrypt the signal.

$$x_{i,j} = z_{i,j} / y_{i,j}^1,\ 1 \le i \le P \tag{12}$$

where $z_{i,j}$ and $x_{i,j}$ are the j-th sample of i-th frame before and after decryption.

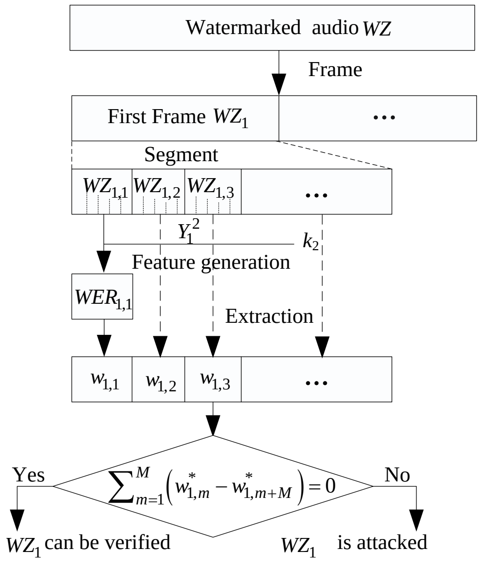

Fig. 2 The process of watermark extraction and content authentication

IV. Performance Analysis and Experimental Results

In this section, 200 WAVE format audio signals are selected as the test signals. They are 16-bit quantified mono signals and sampled at 44.1 kHz. The parameters used are L=120000, N=20, M=3, $k_1 = 0.588$, $k_2 = 0.396$, $\mu = 3.987$. The performance analysis and experimental results are shown in the following subsections.

A. The Security of Watermark Embedding

Some features used for audio watermarking are easily available to attackers. Such as, in order to robust against de-synchronization attacks, some methods embedded synchronization codes in to the host signal. And it was commonly selected signal's energy as the feature for embedding. The computation of the feature (signal's energy) does not require key information, and the feature is easily available to unauthorized users. The unauthorized users can get the quantified feature and extract the synchronization codes. Then they select other signal and embed the same synchronization codes in the selected signal, to substitute the original one. Since the authorizer can extract the correct synchronization codes from the substituted signal, the substitution cannot be detected by the authorizer. If the schemes use the feature easily be acquitted by attackers for watermark embedding, the schemes are vulnerable to substitution attacks.

We take the embedding by quantifying signal's energy as an example to introduce the substitution and attack methods.

We suppose X as the host signal (shown in Fig. 3) and cut the signal into 10 frames. We denote the i-th frame as X_i $(1 \le i \le 10)$ and $W = \{0110110011\}$ as the watermark bits. For a clear introduction to the substitution and attack methods, let's repeat the embedding steps firstly.

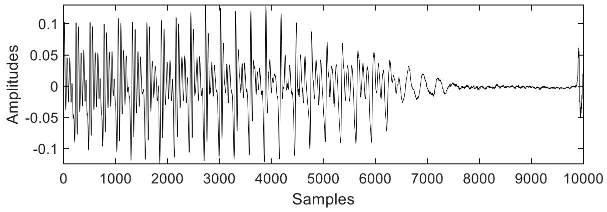

Fig .3 The host signal

1) We calculate the energy of X_1 by using the Eq. (13) and dente the energy as E_1.

$$E_1 = \sum_{l=1}^{N} X_i(l)^2 \tag{13}$$

where $X_1(l)$ is the l-th sample of X_1, and N is the length of X_1.

2) We embed the first watermark bit w_1 ($w_1 \in W$, $w_1 = 0$) by quantifying the energy E_1, using the Eq. (14) . In this section $w_2 = 1$, we should use the Eq. (15) to quantify the energy feature.

$$QE_1 = \begin{cases} \lfloor E_1/\Delta \rfloor \times \Delta + \Delta/2, & T = 0 \\ (\lfloor E_1/\Delta \rfloor - 1) \times \Delta + \Delta/2, & T = 1 \end{cases} \tag{14}$$

$$QE_1 = \begin{cases} \lfloor E_1/\Delta \rfloor \times \Delta + \Delta/2, & T = 1 \\ (\lfloor E_1/\Delta \rfloor + 1) \times \Delta + \Delta/2, & T = 0 \end{cases} \tag{15}$$

In Eq. (14) and (15), Δ and QE_1 are the quantification step and the quantified feature, $T = \lfloor E_1/\Delta \rfloor \bmod 2$. In this section, we set $\Delta = 1$. According to the quantified feature QE_1, we can get the signal that the watermark bit w_1 is embedded, by using the Eq. (16).

$$QX_1 = X_1 \times \sqrt{\frac{QE_1}{E_1}} \tag{16}$$

Repeat the above steps, we can embed other watermark bits w_i into the frames X_i ($2 \le i \le 10$). We denote the watermarked signal as WX, shown in Fig. 4.

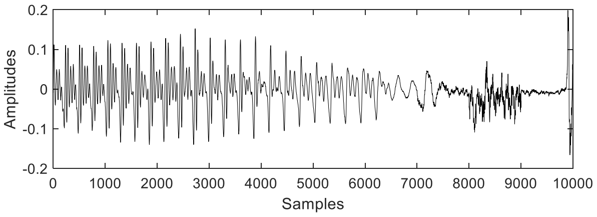

Fig .4 The watermarked signal

The watermarked signal WX and the calculation method of energy feature are known for attackers. They perform substitution attack by using the following steps. We suppose the quantification step Δ is confidential.

1) Attackers cut the watermarked signal WX into 10 frames, WX_i ($1 \le i \le 10$). Then they calculate the energy feature of the 10 frames, which are the quantified feature and denoted by EX_i ($1 \le i \le 10$). The 10 features are shown in Fig. 5. According to the different quantified features, the attackers can calculate the quantification step $\Delta = 1$. In fact, the quantized features have a certain regularity by a fixed quantification step. And the minimal difference between all the quantified energy can be regarded as the quantification step.
2) The attackers can extract all the watermark bits $W = \{w_i | 1 \le i \le 10\}$ ($W = \{0110110011\}$) from the quantized features. w_i can be calculated by using the Eq. (17).

$$w_i = \lfloor EX_i/\Delta \rfloor \bmod 2 \tag{17}$$

3) The attackers select other audio signal, denoted by B, the length of which is same to WX_i (has N samples). They calculate the energy feature of B, and denote

the feature as *EB*.

4) We suppose the attackers select the second frame of watermarked signal to perform substitution attack. They embed the second watermark bit $w_2 = 1$ in the signal *B* by quantifying the energy feature *EB*, using the Eq. (15). Then they can get the signal w_2 embedded, and substitute the second frame (WX_2) of watermarked signal WX, to perform the substitution attack. We show the attacked signal and the energy feature in Fig. 6 and Fig. 7.

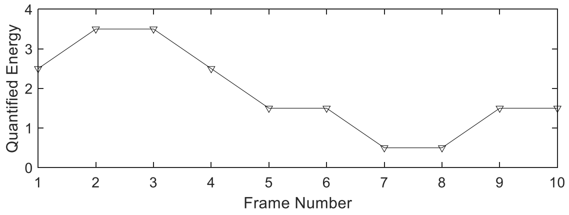

Fig .5 The quantified energy feature

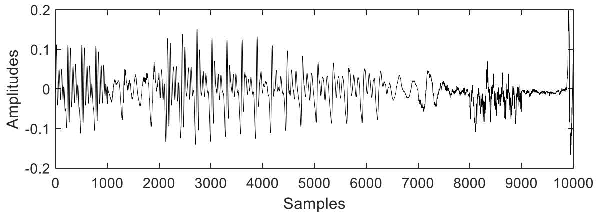

Fig .6 The watermarked signal after being attacked

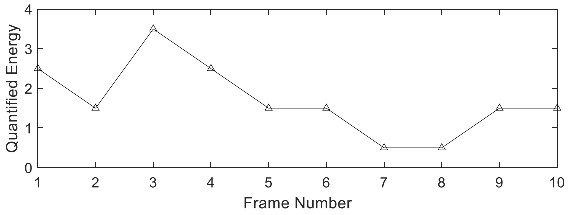

Fig .7 The energy feature of attacked signal

Based on the energy feature shown in Fig. 7, we can get the conclusion that the watermark bits extract from the attacked signal is same to the intact signal. If users verify whether the watermarked signal is attacked by extracting the watermark information, the substitution will not be detected. Based on the analysis, we can get the conclusion that, if the features used for embedding watermark are public, it will bring security risks to the watermarking system.

In this paper, frame number as watermark embedding is by quantifying the signal energy ratio feature. Based on the generation method of the feature (shown in Eq. (1)), it is hard to obtain the feature without the signal Y^2. Y^2 is generated by logistic chaotic mapping, which is related to the secret key k_2. For attackers without the secret key, it's difficult to get the feature for embedding. If attackers select a secret key randomly to perform the substitution attack, the probability that the attacked signal can be verified is $1/10^M$. That is, for the watermark embedding method proposed, the ability against the substitution attack for one frame is

$$A_s = 1 - \frac{1}{10^M} \tag{18}$$

where A_s represents the ability against substitution attack.

Based on the performance analysis above, the abilities of the scheme are compared with those proposed in [12-15], shown in Table I, in which Ability I and Ability II represent the ability resisting to substitution attack and the security of watermark embedding, respectively. The LMC feature defined in [15] is the logarithmic mean of coefficient. From the comparison results, it's concluded that the scheme has the ability resisting to substitution attack, and can improve the security of watermark embedding.

TABLE 1
ABILITY COMPARISON FOR DIFFERENT SCHEMES

Scheme	Features Used	Ability I	Ability II
[12]	Energy (public)	No	No
[13]	Feature points(public)	No	No
[14]	DYWT (public)	No	No
[15]	LMC(public)	No	No
Proposed	Signal energy ratio (secret)	Yes	Yes

B. *Tamper Location*

We select one signal randomly and encrypt the signal. The original audio and the watermarked one are shown in Fig. 8 and Fig. 9. Then we perform deletion attack on the signal (for other attacks, insertion and substitution attack, the tamper location methods and results are similar). The attacked signals and the tamper location results are given in the following.

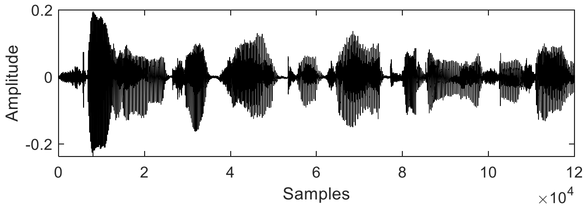

Fig. 8 The original audio

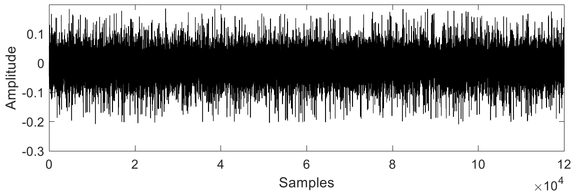

Fig. 9 The watermarked audio

We delete the samples between 20001-th to 30000-th of the watermarked audio (shown in Fig.9). The attacked signal is shown in Fig. 10.

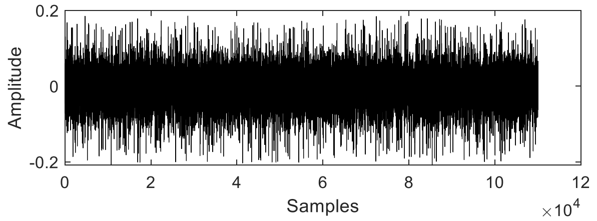

Fig. 10 The attacked signal

--First, by using the method proposed, we can get the first frame (the sample 1 to 6000) is intact. Let's verify frame by frame, and we get the 4-th frame cannot be verified.

--Second, then we move sample, and verify the next *L*/*N* length samples. Until the samples as one frame can be verified. The frame in the middle that cannot be authenticated is the attacked signal. Base on the method, we get the tamper location result shown in Fig. 11, in which FN represents the frame number extracted, and $TL = 1$ represents that the corresponding frame is intact, $TL = 0$ represents that the corresponding frame is attacked.

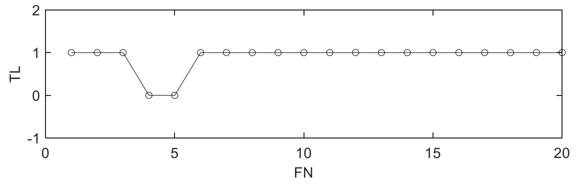

Fig. 11 The tamper location result

--Third, we use 0 amplitude signals to substitute the attacked frame (shown in Fig.12). Then we decrypt and perform reverse scrambling operation on decrypted signal. The result is shown in Fig. 13.

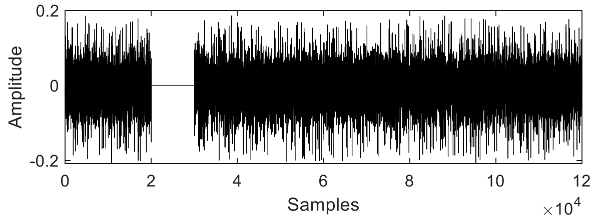

Fig. 12 The signal substituted by 0 amplitude signals

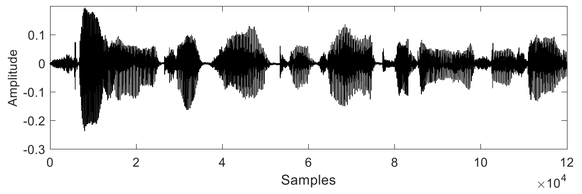

Fig. 13 The decrypted signal

During the experiment, we use 0 amplitude signals to substitute the attacked frames. Firstly, the substitution can make the attacked signal to be synchronized, which is very important for the scrambled signal. If the signal is desynchronized, the signal obtained by anti-scrambling operation will be different from the original one. Secondly, 0 amplitude signals are spread to different parts after anti-scrambling and do not influence the expressed meaning of original signal. So the 0 amplitude signals are selected to substitute the attacked frame. And experiment results also show that by using 0 amplitude signals can improve the usefulness of the algorithm.

V. Conclusion

In this paper, we proposed a watermark scheme for encrypted audio to protect the privacy of audio signals stored on third-party servers. Firstly, we encrypted the audio signal, including scrambling and sample value mapping. And we defined the audio feature signal energy ratio. Then we embedded watermark into the encrypted audio by quantifying the feature and obtained the watermarked audio. Experimental results shown that the scheme can locate the attacked frame. Besides, the scheme can recover the meaning of the attacked audio to some extent. Overall, the scheme improves the security of watermark system and improves the usefulness of watermarking scheme.

References

[1] Y. J. Kuang, Y. Li, P. Li, “A Searchable Ciphertext Retrieval Method Based on Counting Bloom Filter over Cloud Encrypted Data,” IAENG International Journal of Computer Science, vol. 47, no.2, 2020, pp. 271-277.

[2] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, W. J. Lou. “Privacy-preserving public auditing for secure cloud storage,” IEEE Transactions on Computers, vol. 62. no. 2, 2013, pp. 362-375.

[3] N. A. M. Razali, W. N. W. Muhamad, K. K. Ishak, etc., “Secure Blockchain-Based Data-Sharing Model and Adoption among Intelligence Communities,” IAENG International Journal of Computer Science, vol. 48, no.1, 2021, pp.18-31.

[4] Kwok-Wo Wong, Bernie Sin-Hung Kwok, Wing-Shing Law. “A fast image encryption scheme based on chaotic standard map,” Physics Letters, vol. 372. no.15, 2007, pp. 2645-2652.

[5] T. Gopalakrishnan, S. Ramakrishnan. “Image Encryption Using Hyper-chaotic Map for Permutation and Diffusion by Multiple Hyper-chaotic Maps,” Wireless Personal Communications, vol. 109, no. 1, 2019, pp. 437-454.

[6] G. Cheng, C Wang, H Chen. “A Novel Color Image Encryption Algorithm Based on Hyperchaotic System and Permutation-Diffusion Architecture,” International Journal of Bifurcation and Chaos, Vol. 29, no. 9, 2019, pp. 17.

[7] S. Noshadian, A. Ebrahimzade, S. Kazemitabar. “Optimizing chaos based image encryption,” Multimedia Tools and Applications, vol. 77, no. 19, 2018, pp. 25569-25590.

[8] D. Shah; T. Shah; I. Ahamad; M. Haider; I. Khalid. “A three-dimensional chaotic map and their applications to digital audio security,” Multimedia Tools and Applications, vol. 80, no. 1, 2021, pp. 1-23.

[9] I. E. Hanouti; H. E. Fadili, “Security analysis of an audio data encryption scheme based on key chaining and DNA encoding,” Multimedia Tools and Applications, DOI: https://doi.org/10.1007/s11042-021-10592-x.

[10] C. Wang; Q. Ding. “Theoretical design of controlled digitized chaotic systems with periodic orbit of upper limit length in digital circuit,” Nonlinear Dynamics, vol. 98, no. 1, 2019, pp. 257-268.

[11] N. Nagaraj, M. C. Shastry, P. G. Vaidya. “Increasing average period lengths by switching of robust chaos maps in finite precision,” The European Physical Journal Special Topics, vol. 165, no. 1, 2008, pp. 73-83.

[12] B. Y. Lei, I. Y. Soon, Z. Li. “Blind and robust audio watermarking scheme based on SVD-DCT,” Signal Process, vol. 91, no. 8, 2011, pp. 1973-1984.

[13] C. M. Pun, X. C. Yuan. “Robust segments detector for de-synchronization resilient audio watermarking,” IEEE Transactions on Audio, Speech, and Language Processing, vol. 21, no, 11, 2013, pp. 2412-2424.

[14] Y. Wang, S. Q. Wu, J. W. Huang. “Audio watermarking scheme robust against desynchronization based on the dyadic wavelet transform,” Journal of Advances in Signal Processing, vol. 2010, no. 13, 2010, pp. 1-17.

[15] Z. H. Liu, X. L. Zhao, Y. Jin, “Audio watermarking algorithm for tracing the re-recorded audio source,” IAENG International Journal of Computer Science, vol. 48, no. 4, pp1162-1169, 2021.