

DOI: 10.7652/xjtuxb201909015

乱序局部敏感哈希音频零水印方案

滕晓宇^{1,2}, 桂小林^{1,2}, 戴慧珺^{1,2}, 李宗育^{1,2}, 王志通³, 李发兵¹

(1. 西安交通大学电子与信息工程学院, 710049, 西安; 2. 西安交通大学陕西省计算机网络
重点实验室, 710049, 西安; 3. 本钢集团有限公司, 117000, 辽宁本溪)

摘要: 针对现有音频零水印算法缺乏安全分析性研究、构造过程复杂化、唯一性差、未考虑音频帧信息含量分布不均等问题,提出了一种命名为分析重构攻击的特殊攻击模型,并基于该攻击模型结合音频信号小波特征与局部敏感哈希,设计了一种抗分析重构攻击的音频零水印方案。该方案分为零水印构造与零水印检测这 2 大模块:在零水印构造模块,首先提出并设计了去静音帧模型,利用该模型对音频信号进行预处理,从根源上降低水印构造过程中的复杂度,再结合链表、局部敏感哈希以及小波变换构造零水印,最后将水印信息与水印图像结合;在零水印检测模块,通过对水印信息的相似度计算与水印图像的相似度比对共同判断版权归属。为了验证方案有效性及可行性,从方案自身验证与对比分析这 2 方面对方案进行验证分析,理论分析与实验结果表明:该方案所构造的音频零水印最小分析重构复杂度为特征矩阵的平方阶,具有较好的不可感知性、抗噪声攻击性、抗 MP3 压缩攻击性及抗多比例剪裁攻击性等优势。

关键词: 音频零水印;攻击模型;抗分析重构;去静音帧;链表;乱序局部敏感哈希

中图分类号: TP391 **文献标志码:** A **文章编号:** 0253-987X(2019)09-0110-10

Zero-Watermark Scheme for Audio Using Disorder-Locality-Sensitive Hashing

TENG Xiaoyu^{1,2}, GUI Xiaolin^{1,2}, DAI Huijun^{1,2}, LI Zongyu^{1,2}, WANG Zhitong³, LI Fabing¹

(1. School of Electronics and Information Engineering, Xi'an Jiaotong University, Xi'an 710049, China;
2. Shaanxi Province Key Laboratory of Computer Network, Xi'an Jiaotong University, Xi'an 710049, China;
3. Benxi Iron and Steel Group Co. Ltd., Benxi, Liaoning 117000, China)

Abstract: Aiming at the problems such as lack of security analysis, complicated construction process, weak uniqueness, and neglect of considering the audio information content distribution, a special attack model named analysis and reconfiguration attack model is proposed. Based on this attack model, a new scheme of audio zero-watermarking is designed, which combines discrete wavelet transform with locality-sensitive hashing. The scheme contains two main modules of zero-watermarking construction and zero-watermarking detection. In the zero-watermarking construction module, a de-mute frame model for signal is designed. This model uses the attack model to preprocess audio signal for reducing complexity of zero-watermarking construction, and constructs watermark by link list, locality sensitive hash and discrete wavelet transform, then the watermark information and watermark images are combined. In the zero-watermark detection module, the copyright attribution is determined by calculating the similarity of the watermark and

the similarity of the watermark images. Finally, the effectiveness and feasibility of this new scheme are verified via self-verification and comparative analysis. Theoretical analysis and experimental results demonstrate that this scheme can construct an audio zero-watermark with minimum analysis and reconfiguration complexity of square order of eigenmatrix, and has the advantages of good imperceptibility, robustness, and capabilities of resisting MP3-compression attack and multi-proportional tailoring attack.

Keywords: audio zero-watermark; attack model; anti-analysis and reconfiguration; de-mute frame model; link list; disorder-locality-sensitive hashing

信号处理技术的普及使得多媒体作品的复制、篡改操作变得极为容易和隐蔽^[1],此类问题在音频信号中尤为严重。数字水印技术作为多媒体安全研究的一个分支^[2],以其隐蔽性高、安全性好等优点,已经成为解决此类问题较为简单和通用的方法之一。

音频数字水印按照嵌入方式分为嵌入式水印与零水印。嵌入式水印以牺牲水印信息嵌入量与音频质量为代价,通过更改原始音频的时域或频域信息来嵌入水印^[3-4]。零水印算法根据音频信号的特征向量构造水印,并不向原始音频信号中添加任何信息,即对音频信号零更改,因而能够较好地处理数字水印的透明性与鲁棒性之间的关系^[5-7]。

目前,针对音频的零水印算法已有不少研究成果,大致可以分为以下3类:①单纯型,该方法根据单一的音频信号特征如倒谱系数、小波域特征、短时能量、过零率等直接构造水印^[8-9],具有良好的时间特性,但构造算法易被破解;②多特征混合型,该方法结合信号特征与信号处理方法构造音频水印^[10-13],提高了水印的鲁棒性但增加了构造算法的复杂度,而且并未考虑到水印信息的安全性;③双水印算法,该方法将以上2种零水印构造结果相融合,得到最终的水印信息^[14-15],在一定程度上降低了暴力破解水印信息的概率,但不能确保一定会增强水印信息的鲁棒性,而且同时增大了算法复杂度。

综上所述,现有的音频零水印算法虽然能满足一般情况下对音频零水印的需求,但仍旧存在以下不足:①高性能的数字音频水印算法总是以牺牲算法复杂度为代价的;②由于未考虑音频信号中每帧信息含量的差异性,导致算法运行过程中存在大量冗余工作;③不能保证水印信息的唯一性;④忽略了水印信息的安全性,即可通过构造出的水印信息破解水印构造算法。

为此,本文在分析总结现有的音频零水印的基础上,从安全性的角度提出了一种针对水印信息的攻击模型,并以此为基准设计了一种基于乱序局部

感知哈希的音频零水印方案。

1 分析重构攻击模型及零水印方案设计

1.1 分析重构攻击模型

分析重构攻击模型定义在音频零水印领域,是以水印信息安全性为出发点的一种特殊的攻击,具体表现为当发生水印信息泄漏时,只需通过分析泄漏的水印信息,即可得知构造水印的元素及方法,从而重构水印算法。分析重构攻击模型实质上是水印构造的逆推导过程。

该种攻击的危害主要表现为以下2点:①在微观上,分析重构出水印信息的过程中同时破解了水印的构造算法,攻击者可以根据水印构造算法在不更改版权信息的情况下篡改、复制原始音频;②在宏观上,版权判定中将无法判定版权信息,致使通过水印判定版权的算法失效,甚至导致整个版权保护系统瘫痪。

分析重构攻击的特点可分为以下4类:①水印信息与原始音频信号的基本特征相似度极高,该种情况大多出现在单纯型水印构造算法中,例如水印信息与在某阈值下的短时平均能量一致;②水印信息与经过多种信号处理的原始音频特征相似,例如水印信息与经过小波分解的短时能量相似;③水印信息与音频信号的组合特征比较相似,该种方式常见于多特征混合型零水印构造算法;④结合多种处理方式,处理通过多种音频信号特征生成的特征向量,该种情况较前3种具有较好的抗分析重构性。

设 $\omega = \{\omega_1, \omega_2, \dots, \omega_n\}$ 表示音频信号的 n 类处理方式, $v = \{v_1, v_2, \dots, v_m\}$ 表示音频信号的 m 类特征,则上述4种分析重构类型中的最小时间复杂度为 $O(1)$,最大时间复杂度为 $O(m!n!)$ 。由于常见的信号处理方式与数字音频特征是无穷可数的,也就是说可以暴力破解水印构造方法。

1.2 符号定义

本文涉及的不同符号及其含义如表1所示。

表 1 符号对照表

处理过程	符号	含义
零水印构造	W	原始音频片段
	V	原始音频的特征向量
	Z	原始音频构造的水印信息
	T	原始音频构造的水印图像
零水印检测	W_1	待检测的音频片段
	V_1	待检测音频的特征向量
	Z_1	水印二次构造所得水印信息
	T_1	待检测音频的水印图像
分帧	L	音频段的长度
	I	帧的长度
	N	采样点数组
	N_w	分帧后音频集合
去静音帧	F	音频信号振幅
	S	振幅的方差
	E	短时平均能量
	M	能量平均值
局部敏感哈希	q	音频帧分帧帧长
	H	哈希函数族
	A, A_1, A_2	局部感知哈希映射数组
	list1, list2	链表
水印图像构造	t	置乱后的图像
	r	置乱阶数
复杂性对比	m	音频信号特征种类数量
	n	音频信号处理方式数量
	R	特征矩阵的行数或列数 (本文设定矩阵为方阵)

1.3 音频零水印方案

音频零水印方案分成零水印构造与零水印检测 2 个部分:零水印构造是根据音频信号的特征向量构造水印;零水印检测是当发生版权纠纷时,对待检测的音频进行水印的二次构造,将构造的结果与原始音频的水印通过相似度检测等手段,判断并确定版权的归属。

由于离散小波变换具有多尺度与多分辨率的特性^[5],能由粗及细地逐步分析信号特征,将其应用到音频零水印中,能保证水印具有良好的鲁棒性。局部敏感哈希^[16-18]的原理是原始相似度较高的两个向量,经过哈希转换之后仍旧具有很高的相似度,而本身不相似的两个向量,经过哈希转换之后同样不相似。将其应用到音频零水印中,能在保证水印结果的准确性的同时增强水印信息的安全性。链表在

数据置换过程中可以起到记录置换顺序,即保序的作用,应用到音频零水印构造过程中可以使水印信息达到更好的抗分析重构性以及唯一性。因此,本文结合音频信号的小波特征与局部敏感哈希以及链表,设计并实现了一种乱序局部敏感哈希的音频零水印方案。

本文提出的零水印方案分为零水印构造模型与零水印检测模型。零水印构造模型主要分为 3 个部分:第 1 部分为音频信号预处理过程,通过对音频信号进行预加重、补帧以及去静音帧等操作,完成音频帧的筛选,从根源上降低音频帧的处理数量,从而达到降低水印构造算法复杂度的目的;第 2 部分为水印的构造过程,通过音频信号的小波分解得到特征向量 V ,根据局部感知哈希族函数 H 将向量进行映射,最后借助链表将哈希变换所得的值进行置乱,从而得到构造的水印信息 Z ,在该部分中,为保证水印信息的唯一性,本文利用链表将哈希映射结果进行置乱,以达到降低水印碰撞性的目的;第 3 部分为水印图像构造,引入水印图像的目的是使得后续水印检测结果更加清晰,该部分借助图像置乱算法将原始图像进行置乱,并与第 2 部分所构造的水印信息相结合,得到水印图像 T 。本文提出的音频零水印构造模型如图 1 所示。

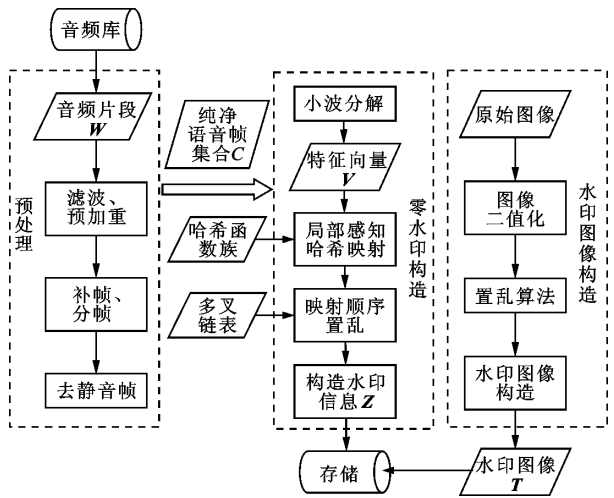


图 1 零水印构造模型

预处理部分在改进现有的通用分帧模型的基础上提出了去静音帧模型,其目的为根据音频信号基本特征去掉信号中静音帧及信息含量较低的部分。令 $\max$ 为取数值集合的最大值操作, $\min$ 为取数值集合的最小值操作, mean 为取数值集合的平均值, S 为振幅 F 的方差, E 为音频信号短时平均能量, S_F 为归一化方差, E_n 为归一化短时能量, Z_n 为 S_F 与

E_n 之比,则筛选过程中涉及到的计算式有

$$S_F = \frac{S - \text{mean}(S)}{\max(S) - \min(S)} \quad (1)$$

$$E_n = \frac{E - \max(E)}{\max(E) - \min(E)} \quad (2)$$

$$Z_n = \frac{S_F}{E_n} \quad (3)$$

由以上分析以及式(1)~(3),可得去静音帧模型如图 2 所示。

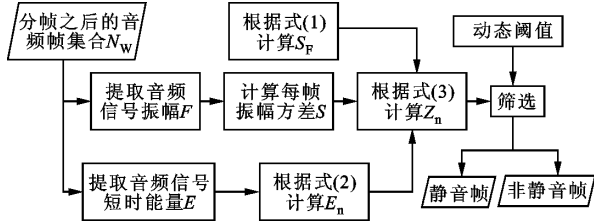


图 2 去静音帧模型

水印图像构造阶段主要分为图像二值化、Arnold 图像置乱^[19]以及水印图像与水印信息结合共 3 个部分,其模型如图 3 所示。

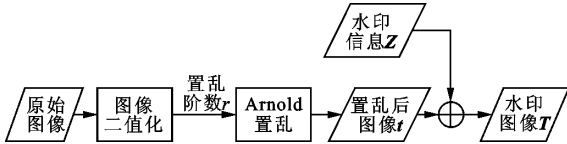


图 3 水印图像构造模型

与零水印构造模型相对应的是零水印检测模型,检测模型同样主要分为 3 个部分:第 1 部分为水印的二次构造,该部分是对待检测的音频片段 W_1 进行水印构造,构造过程中应用到的构造算法与水印构造过程中设计的算法相同(构造过程如图 1 所示),因此该过程为水印二次构造;第 2 部分为相似度计算与相似度比对,前者是针对水印信息 Z 与 Z_1 ,后者是针对水印图像 T 与 T_1 ;第 3 部分是版权判定,根据第 2 部分的结果判定版权的最终归属。音频零水印的检测模型如图 4 所示。

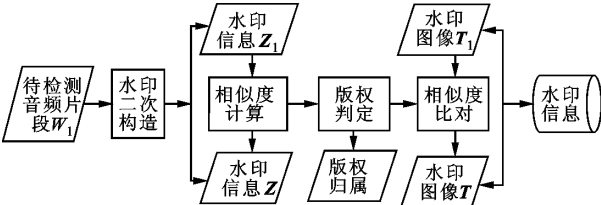


图 4 音频零水印检测模型

在零水印检测过程中,需要对水印图像进行相似度比对,主体为原始图像、存档的水印图像 T 以及经过水印二次构造所得到的待检测音频特征向量 V_1 ,主要理论依据为两次异或等于原始数值这一逻辑关系,具体处理过程如图 5 所示。

辑关系,具体处理过程如图 5 所示。

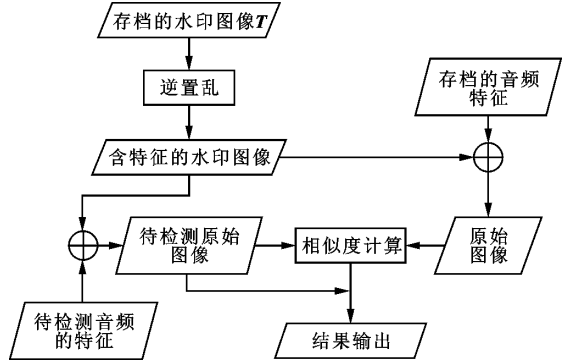


图 5 水印图像比对

2 零水印方案中关键模块算法及设计

由图 1 与图 5 可以看出,实现音频零水印方案的关键模块主要由分帧、去静音帧、特征向量生成、乱序局部敏感哈希水印生成、水印图像构造等组成。

2.1 改进的音频分帧算法

预处理部分主要完成音频信号滤波、预加重、分帧、去静音帧等操作,其中滤波与预加重等前期处理技术的研究已较为成熟,此处不再赘述。

对于分帧算法,文献[20]给出了一种 0 填充分帧方法,该方法提取特征向量时不会影响端点帧的判断。但是,本文设计的零水印构造算法是基于能量值相关的基础运算,现有的分帧方法需改进后方可适用,改进后的音频分帧算法如下:先计算音频段总长度 L 对于帧长 I 的余数 K ,判断 K 与 0 的关系;然后统计第 1 帧与最后 1 帧中 0 的数目,分别用 N_1 与 N_2 表示;再根据 N_1 与 N_2 的大小关系进行 0 填充,最终得到分帧后的语音帧集合 N_w 。本文设计的分帧算法 pro-enframe 的伪代码如下,文献[20]的原始分帧算法在本文设计的算法中以“分帧操作”字样体现。

PROC pro-enframe(L, I, N_1, N_2, N_w)

INPUT:音频段长度 L ,分帧长度 I

OUTPUT:分帧后音频集合 N_w

BEGIN

$K \leftarrow L \% I$; /* 取余运算 */

IF ($K=0$) THEN 分帧操作,得 N_w ;

/* 统计采样点数目 */

For $i \leftarrow 0$ To $I-1$ DO

 【IF $N[i]=0$ THEN $N_1=N_1+1$;】

For $i \leftarrow L-I-1$ To $L-1$ DO

 【IF $N[i]=0$ THEN $N_2=N_2+1$;】

```

IF( $N_1 \geq N_2$ ) THEN
    音频最前补帧并分帧操作;
ELSE 音频最后补帧并分帧操作;
END

```

2.2 特征向量生成

该模块主要完成零水印构造中特征向量的生成,简化了文献[21]关于小波能量的算法,过程为:首先对音频进行小波变换得数组 $D_1[1, \dots, n]$ 、 $D_2[1, \dots, n]$ 、 $D_3[1, \dots, n]$;然后取3个数组中的最大元素作为特征值写入数组 $V[1, \dots, n]$ 中。本文设计的特征向量生成算法 get-vec 的伪代码如下。

```

PROC get-vec ( $N_w, D_1, D_2, D_3, V$ )
INPUT: 音频信号帧集合  $N_w$ 
OUTPUT: 特征向量  $V$ 
BEGIN
     $D_1, D_2, D_3 \leftarrow N_w / \text{小波变换} \times /$ 
    For  $i \leftarrow 0$  To  $I-1$  DO
         $[V[i] \leftarrow \text{MAX}(D_1[i], D_2[i], D_3[i])]$ 
    END

```

2.3 乱序局部敏感哈希水印生成

该模块主要由4部分组成。第1部分为哈希映射选择哈希函数族 H ,此处每一个哈希函数就是一个简单的阈值函数,在对原有特征向量进行降维的同时对数据进行二值化,阈值函数采用动态选取方式,根据数据的平均值并结合随机数函数进行构造。第2部分为局部敏感哈希映射,将每一个特征向量经过哈希映射后的结果组成数组 A 。由于每一个感知哈希函数 h_n 都对应着一个桶 T_n ,每个桶都可以用一个一维数组表示,为方便后续水印图像处理,数组长度应与图像数组行(或列)相等。第3部分为提高水印信息的抗分析重构性,对映射数组 A 进行纵向置乱,并由链表 list1 记录数组 A 中每个向量的首元素在 A_1 中位置。第4部分为置乱映射数组,根据第3部分的方法,将数组 A_1 横向置乱,并由链表 list2 记录每维元素的位置。本文设计的乱序局部敏感哈希水印生成算法 ZL-W 的伪代码如下。

```

PROC ZL-W ( $V, H, A, A_1, \text{list1 list2}$ )
INPUT: 音频特征向量  $V$ 
OUTPUT: 水印信息  $Z$ 
BEGIN
    Step1: 选择哈希函数族  $H$ ;
    Step2:  $A \xleftarrow{\text{映射}} H(V)$ ;
    /* 进行局部感知哈希函数映射,得数组  $A \times /$ 

```

```

Step3:  $A_1 \xleftarrow[\text{list1记录}]{\text{横向置乱}} A$ ;
/* 纵向置乱数组  $A$  得  $A_1$ ,链表 list1 记录 */
Step4:  $Z \leftarrow (A_2 \xleftarrow[\text{list2记录}]{\text{横向置乱}} A_1)$ ;
/* 横向置乱数组  $A_1$  得  $A_2$ ,链表 list2 记录 */
Step5: 输出水印信息  $Z$ 
END

```

哈希函数族 H 生成时,阈值函数是依据待处理数据的平均值来进行选取的。文献[22]表明,阈值选取过程中均值居多,但均值不能较好地满足多峰值信号要求,因此需要引入缩放因子。基于以上分析,本文选取的阈值函数的变化范围为

$$\frac{1}{3} \text{abs} \left[\text{mean} \left(\frac{x - \max(x)}{\max(x) - \min(x)} \right) \right] \sim \frac{1}{2} \text{abs} \left[\text{mean} \left(\frac{x - \max(x)}{\max(x) - \min(x)} \right) \right] \quad (4)$$

式中: x 为感知哈希函数待处理的数据;abs 为取绝对值; $\frac{x - \max(x)}{\max(x) - \min(x)}$ 为对 x 进行归一化处理。

链表 list1 与 list2 的作用是辅助置乱与记录原始顺序。借鉴文献[23]中的方法,用 D_i 表示第 i 维特征向量。图6是零水印构造中的纵向置乱示意图。

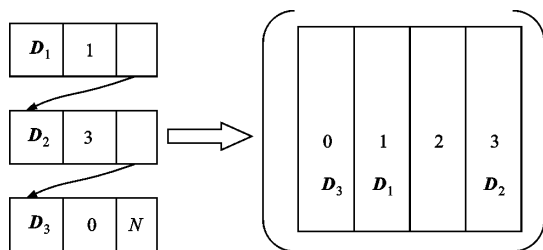


图6 零水印构造中的纵向置乱示意图

从图6可以看出:根据链表结构可以将特征向量置乱,原始水印特征向量的顺序应为 D_1, D_2, D_3 ,经过置乱之后变成 D_3, D_1, D_2 ,而且置乱为无规律置乱,因此在一定程度上增强了水印信息的抗分析重构性。

设数组 $A_1[], B[1, \dots, m][1, \dots, n], C[1, \dots, m][1, \dots, n]$ 、链表 list1 分别存储首元素所在位置、置乱前特征向量、置乱后特征向量、纵向置乱顺序。本文设计的纵向置乱算法 Ra_Z 的伪码如下。

```

PROC Ra_Z( $A_1, B, C, \text{list1}$ )
INPUT: 置乱前的数据  $B$ 
OUTPUT: 置乱后的数据  $C$ ,链表 list1,首元素
        存储数组  $A_1$ 

```

BEGIN

```

 $h \leftarrow d-1$ ;
/* 生成  $d$  个不同的随机数 */
For  $i \leftarrow 0$  To  $d-1$  Do  $[N_L[i] \leftarrow i];$ 
While ( $h \neq 0$ )
     $[V_3 \leftarrow \text{Random}(0, h);$ 
    /* 在  $0 \sim h$  之间随机生成 1 个整数 */
     $g \leftarrow N_L[h]; N_L[h] \leftarrow V_3; N_L[V_3] \leftarrow g;$ 
    /* 交换数据 */  $h \leftarrow h-1;$ 
/* 根据随机数置乱特征值,并由 list1 记录 */
 $p \leftarrow 0$ ; /* 用于指示数组值 */
 $A_1 \leftarrow N_L[1];$ 
For  $i \leftarrow 0$  To  $n-1$  Do
     $[W_L \leftarrow N_L[i];$  /* 取出随机数值 */
     $C[i][i] \leftarrow B[i][p];$ 
    list1.data  $\leftarrow p$ ;
    list1.link  $\leftarrow N[i+1]; p \leftarrow p+1;$ 
END

```

2.4 水印图像构造

该模块主要完成零水印构造过程中水印图像的构造,由图3水印图像构造模型以及文献[17]图像置乱算法组成,水印信息构造以帧为单位,水印图像的选取是与帧数相对应,以便构造水印图像。设 Y 为原始图像, r 为图像置乱的阶数, Z 为水印信息, t 为置乱后的图像, T 为最终得到的水印图像,本文设计的水印图像构造算法 Water-P 的伪代码如下。

PROC Water-P (Y, r, Z, t, T)

INPUT: 原始图像 Y , 置乱阶数 r , 水印信息 Z

OUTPUT: 水印图像 T

BEGIN

```

 $Y_2 \xleftarrow{\text{图像二值化}} Y;$ 
/* 对原始图像二值化处理,得到图像  $Y_2$  */
 $t \xleftarrow{r \text{ 阶 Arnold 置乱}} Y_2;$ 
 $T \leftarrow t \text{ XOR } Z;$ 
/* 将水印信  $Z$  与图像  $t$  进行按位异或操作 */
输出水印图像  $T$ ;
END

```

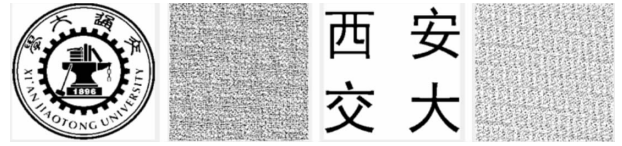
3 实验验证及对比分析

由于本文提出的音频零水印方案是针对抗分析重构攻击的,因此方案的分析验证应分为自身可行性验证分析以及与其他方案对比分析共2个部分,前者侧重于验证,后者侧重于对比分析。

3.1 实验数据选取

本文的实验数据主要分为音频数据和水印图像数据2个部分。音频数据分为语音数据与音乐数据,语音数据部分采用的是麻省理工大学的公开数据库 TIMIT、以汉语普通话形式录制的男女声发音“0~9”、连续语音“西安交通大学电子与信息工程学院”,而音乐数据主要选用中国古典民族器乐片段。

为增强版权判定结果的可阅读性与直观性,本文引入水印图像,由于单纯的黑体字样图像不能很好地体现细微的图像变化,因此本文在水印图像的选取阶段同时采用印有西安交通大学校徽的图像和印有“西安交大”黑体字样的图像作为原始水印图像,二值化后的水印图像以及3阶置乱后的效果图如图7所示。



(a) 校徽二值图像 (b) 校徽图像置乱效果图 (c) 黑体字的二值图像 (d) 黑体字图像置乱效果图

图7 二值水印图像及置乱效果图

3.2 方案验证分析

筛选方案的分析验证从不可感知性、可行性、有效性等方面展开。

3.2.1 水印的不可感知性 水印是否被感知是指嵌入水印信息前后的音频段是否发生改变,以及这种改变能否被人耳感知。本文采用零水印方式,从音频信号中提取特征用以构造水印,并未向原始音频信号中添加任何信息,即对原始音频信号零改变。图8为采用本文提出的音频水印方案嵌入水印前后的时域波形对比,从图中可以看出,嵌入水印前后信号的差值恒为0,即嵌入水印前后信号完全相同,因此本文方案具有良好的不可感知性。

3.2.2 去静音帧算法有效性验证 为了验证去静音帧算法的有效性,本文选取连续语音“西安交通大学电子与信息工程学院”作为验证对象,此处音频帧的帧长 $q=256$,筛选阈值为-0.35,筛选效果如图9所示。

由于图9a时域波形较为密集,因此仅选出2个具有代表性的区域,对去静音帧效果进行说明。图9b中①②区域对应图9a中静音或者带有部分噪声的区域①②,可以看出,在图9a中区域①②所对应的时域波形几乎聚集在0附近,即所对应的数据帧

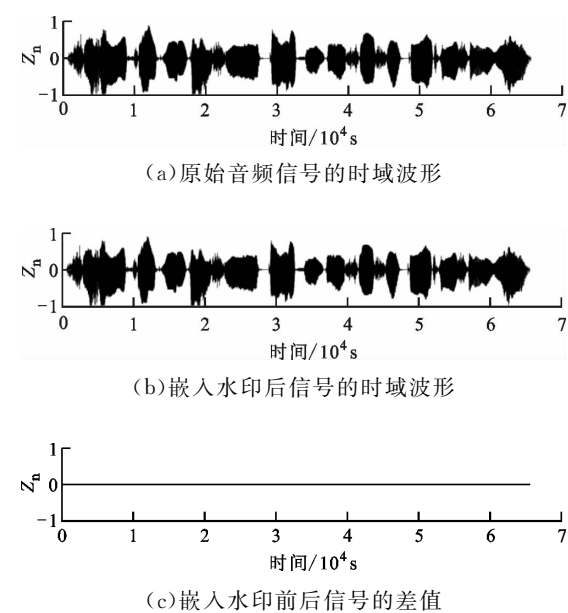


图 8 嵌入水印前后的音频时域波形对比

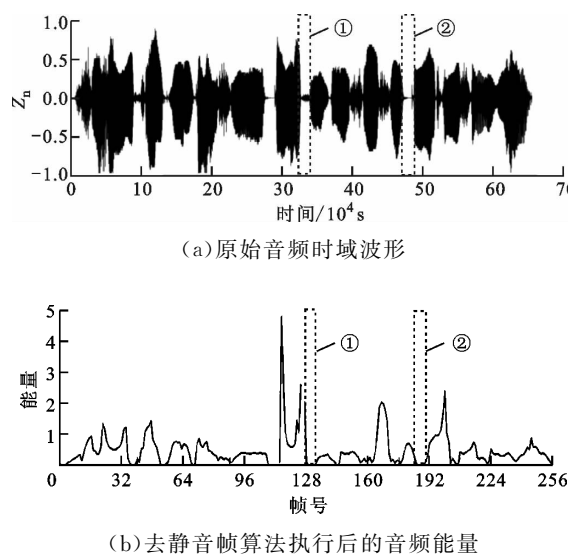


图 9 去静音帧算法的效果验证

为静音帧或者信息含量低,所以对应在图 9b①②中为 0。因此,本文的去静音帧算法是有效的并且合理的。

3.2.3 零水印构造方案验证 以连续女声发音“西安交通大学电子与信息工程学院”为验证用例来验证零水印构造方案是否可以有效执行,水印构造前后效果具体如图 10 所示。

根据本文提出的零水印构造方案可知,在待检测语音的特征向量与原始语音的特征向量相似度较高的情况下,可以完全恢复无噪声水印图像。从图 10b、10c 与图 10e、10f 可以看出,从待检测音频可还原清晰可见的原始水印图像。当加入强背景音乐后,二次构造的水印图像如图 11 所示,可以看出,2

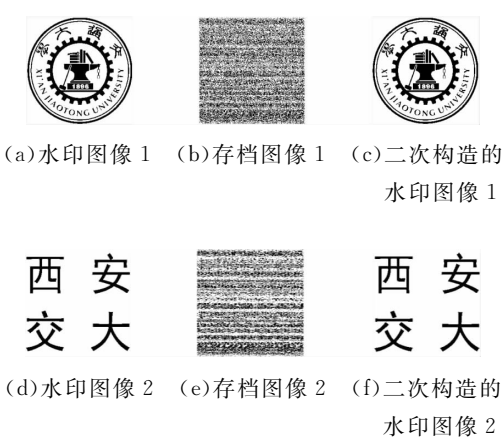


图 10 水印构造前后效果图

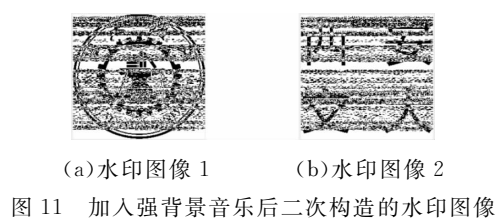


图 11 加入强背景音乐后二次构造的水印图像

幅水印图像几乎已经无法辨别校徽与黑体汉字。因此,本文所提出的音频水印方案是可行的。

3.3 方案对比分析

为了进一步验证本文提出的音频零水印方案的有效性,从可行性、鲁棒性与抗分析重构性这几个方面与相关研究进行对比分析。

3.3.1 抗分析重构性 文献[1]是基于特征的双水印,采用混沌方式将水印图像进行置乱,使得水印信息无法从图像中读出,但未对水印特征向量采取保护措施,一旦秘钥泄漏,水印图像以及水印信息将被成功解密。本文与其设计思路不同,通过置乱水印特征信息来增强抗分析重构性。

设 m 为音频信号特征的种类数量, n 表示处理方式种类数, R 表示需要构造特征矩阵的行数与列数,并且 $n < R, m < R$ 。将本文提出的置乱敏感哈希水印方案分别与文献[5,8-9]在分析重构复杂度方面进行分析比较,结果如表 2 所示。

表 2 分析重构复杂度对比

方案来源	最大时间复杂度	最小时间复杂度
文献[5]	$O(m^2n)$	$>O(1)$
文献[8]	$>O(mn)$	$>O(1)$
文献[9]	$>O(mn^2)$	$>O(1)$
本文	$O(R! R! m)$	$>O(R^2)$

从表 2 可以看出,本文提出的乱序局部敏感哈希零水印方案的抗分析重构性明显高于文献[5,8-

9]的算法,具有良好的抗分析重构性。

3.3.2 鲁棒性 为方便对比分析,采用归一化相关系数 C_N 作为算法鲁棒性的评价指标,计算公式为

$$C_N(\mathbf{Z}, \mathbf{Z}_1) = \frac{\sum_{i=1}^{L_1} \sum_{j=1}^{L_2} Z(i, j) Z_1(i, j)}{\sqrt{(\sum_{i=1}^{L_1} \sum_{j=1}^{L_2} Z^2(i, j)) (\sum_{i=1}^{L_1} \sum_{j=1}^{L_2} Z_1^2(i, j))}} \quad (5)$$

式中: L_1 表示水印每维向量的大小; L_2 表示水印向量的维数。 $L_1 \times L_2$ 即为水印信息的大小。 C_N 越大表示鲁棒性越好。

本文从抗噪声攻击、抗 MP3 压缩攻击、抗多种比例裁剪攻击这 3 方面进行方案鲁棒性的分析比对。

(1)抗高斯噪声攻击。对原始音频信号分别添加均值为、标准方差为 0.000 3 与均值为、标准方差为 0.000 5 的高斯白噪声,并分别与文献[1](嵌入水印)、文献[5]、文献[24]进行比对分析,结果如表 3 所示。

表 3 不同方案在不同攻击强度下的鲁棒性评价

方案来源	C_N	
	方差为 0.000 3	方差为 0.000 5
文献[1]	0.985	0.981
文献[5]	0.993	0.990
文献[24]	0.983	0.974
本文	0.994	0.990

由表 3 可知:本文提出的音频零水印方案在 2 种攻击强度下的 C_N 明显大于文献[24]的结果,略大于文献[1]的结果,由于本文与文献[5]都采用了小波变换,因此在抗噪性方面与文献[5]处于几乎持平状态。综上可知,本文提出的零水印构造方案有较好的抗噪声攻击性。

(2)抗 MP3 压缩攻击。MP3 压缩是指通过一定的速率将原始文件压缩成较小的文件,在这个过程中,器乐相对于语音较为敏感。对原始器乐《凤凰于飞》片段分别进行速率为 96、128、160 kb/s 的压缩攻击,并与文献[5]和文献[24]进行对比分析,结果如下:由于本文与文献[5]、文献[24]都涉及离散小波变化,所以在抗 MP3 压缩攻击上性能差异不大, C_N 几乎持平;3 种方案在不同的压缩速率下, C_N 都能保持在 0.9 以上,都在压缩速率为 128 kb/s 时达到最大值,此时 $C_N \geq 0.98$;由于压缩速率为 96 kb/s 时采用的是低频压缩,原始器乐的高频段的一部分丢失,水印构造产生会受到影响,3 种方案的抗

MP3 压缩攻击性都不太好。因此,本文所提出的音频零水印构造方案具有一定的抗 MP3 压缩攻击能力。

(3)抗剪裁攻击。抗剪裁攻击是指将原始音频的部分信息裁剪掉后,仍可以进行版权判定,是水印信息鲁棒性的一个重要体现。选取汉语连续语音“西安交通大学电子与信息工程学院”以及单音男女发音“0~9”进行剪裁攻击实验,并与文献[1]、文献[5]、文献[24]进行对比。

剪裁攻击选取的帧数为

$$C = \lfloor \mu L_{\text{num}} \rfloor \quad (6)$$

式中: C 为剪裁攻击中需要被剪裁的帧数; μ 为剪裁攻击比例; L_{num} 为攻击目标的总帧数; $\lfloor \cdot \rfloor$ 为向下取整。

攻击中需要剪裁的帧序号为

$$A_N = \text{rand}(C, L_{\text{num}}) \quad (7)$$

式中: A_N 为需要剪裁的帧序号; rand 为随机数生成函数。

在式(7)生成随机数的过程中,如果随机生成所得的静音帧比例高于一定阈值,则需要重新进行生成。由于语音段中静音帧的比例较高,阈值通常先选为 50%,再根据具体语音进行调整。器乐段中静音帧比例较低,通常选为 67%(2/3)。

在实验对比之前首先对本文提出的零水印方案进行剪裁攻击,效果如图 12 所示。

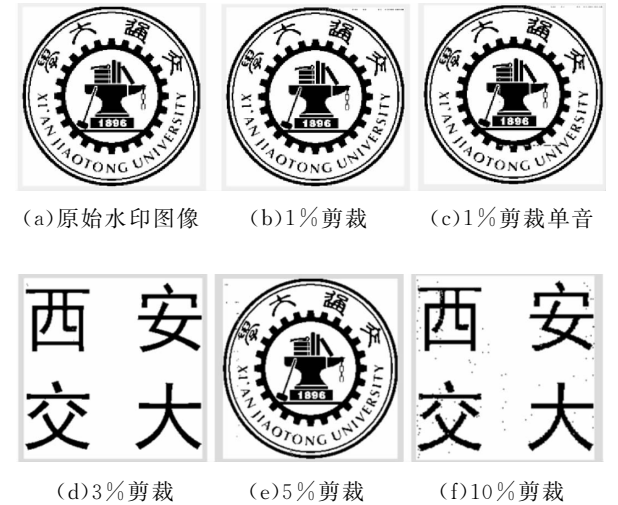


图 12 本文方案剪裁攻击后二次构造的水印图像

图 12a 为原始水印图像;图 12b 为连续语音(女)在攻击强度为 1%时二次构造的水印图像;图 12c 为单语音在攻击强度为 1%时二次构造的水印图像;图 12d 为英语语音在攻击强度为 3%时二次构造的水印图像,英语语音为 TIMIT 数据库中任

取的1条语音;图12e为中国古典民族器乐《凤凰于飞》片段在攻击5%时二次构造的水印图像;图12f为连续语音(男)在攻击强度为10%时二次构造的水印图像。从图中可以看出:本文提出的方案在攻击强度为5%时才出现明显的噪声,如图12e所示;在强度为10%时,虽然噪声已经很明显,但是水印图像信息仍旧清晰,如图12f所示。

选取汉语男女发音语音为用例进行剪裁攻击实验,并与文献[1]、文献[5]以及文献[24]进行比对分析,由于本文采用一定比例的随机剪裁,相同比例下对应的剪裁的位置是不一样的,所以每种剪裁比例分别对应5组实验,其平均 C_N 如图13所示。

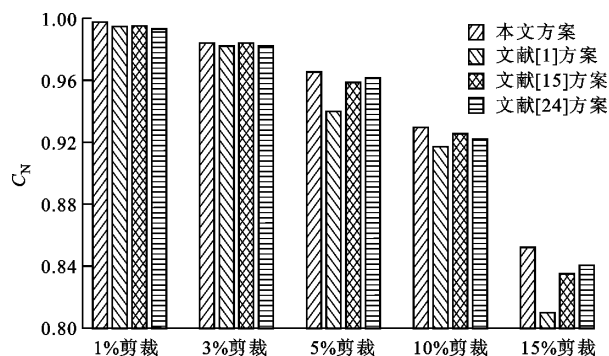


图13 不同方案在不同攻击强度下的 C_N

由图13可知:当攻击强度小于3%时,4种方案相差不大;随着攻击强度的增大,4种方案都存在下降趋势,文献[1]为嵌入水印,因此下降最快,而本文方案下降较慢,略好于其他方案。因此,本文方案具有较好的抗剪裁攻击性。

4 结 论

本文通过对音频零水印技术的现状进行分析,从安全角度入手,提出了一种分析重构水印攻击模型,并依据此攻击模型提出了一种基于乱序局部敏感哈希音频零水印方案。该方案主要分为两大模块:零水印构造和零水印检测。零水印构造过程中主要借助局部敏感哈希以及链表增强水印信息的抗分析重构性。在零水印构造模块中:在预处理阶段根据音频信号的特点设计了去静音帧模型,从源头降低了水印构造算法的时间复杂度;在水印构造过程中,结合链表、局部敏感哈希以及小波变换共同设计构造模型,并将水印信息与水印图像相结合。在零水印检测模块中,对待检测音频依据本文提出的水印构造算法进行水印的二次构造,之后经过相似度计算和与水印图像的相似度比对判定版权的归属。理论分析与对比实验表明,本文提出的零水印

方案能在保持较低计算复杂度的情况下仍具有良好的抗分析重构性与鲁棒性。但是,本文的特征提取仅从小波分析入手,特征单一,在一定程度上会造成版权判定过程中准确度下降、抗噪性差。与此同时,局敏感哈希与链表结合会造成复杂度高、可读性差。这都是下一步需要改进的地方。

参考文献:

- [1] 韩颖铮, 邓国强. 基于置乱加密和 DWT 的音频双水印算法 [J]. 电子设计工程, 2018, 26(12): 153-156.
HAN Yingzheng, DENG Guoqiang. An audio dual watermarking algorithm based on scrambling encryption and discrete wavelet transform [J]. Electronic Design Engineering, 2018, 26(12): 153-156.
- [2] 肖迪, 马青青, 王兰, 等. 基于稀疏表示的云协助安全数字水印技术 [J]. 信息网络安全, 2017(1): 1-7.
XIAO Di, MA Qingqing, WANG Lan, et al. Cloud-assisted secure digital watermarking based on sparse representation [J]. Netinfo Security, 2017(1): 1-7.
- [3] XIANG Y, NATGUNANATHAN I, PENG D Z, et al. Spread spectrum audio watermarking using multiple orthogonal PN sequences and variable embedding strengths and polarities [J]. ACM Transactions on Audio, Speech, and Language Processing, 2018, 26(3): 529-539.
- [4] 王浩, 陈砚圃, 高悦, 等. 基于扩频的数字音频水印技术研究 [J]. 现代电子技术, 2012, 35(2): 7-9.
WANG Hao, CHEN Yanpu, GAO Yue, et al. Investigation of digital audio watermarking technology based on spread spectrum [J]. Modern Electronics Technique, 2012, 35(2): 7-9.
- [5] 宋慧, 李晨, 田丽华. 基于音频特征 MFCC 的零水印算法 [J]. 计算机应用与软件, 2016, 33(10): 140-144.
SONG Hui, LI Chen, TIAN Lihua. Zero-watermarking algorithm based on audio features of MFCC [J]. Computer Applications and Software, 2016, 33(10): 140-144.
- [6] TANG X, MA Z F, NIU X X, et al. Compressive sensing-based audio semi-fragile zero-watermarking algorithm [J]. Chinese Journal of Electronics, 2015, 24(3): 492-497.
- [7] TSAI S M. A robust zero-watermarking scheme for digital audio [J]. International Journal of Information and Electronics Engineering, 2015, 5(2): 117-121.
- [8] 张兵路, 姜建国, 冯复科. 基于 DWT 的音频“零数字”水印技术研究 [J]. 计算机工程, 2005, 31(18): 148-

- 149, 152.
- ZHANG Binglu, JIANG Jianguo, FENG Fuke. Study of audio zero-digital watermarking technology based on DWT [J]. Computer Engineering, 2005, 31(18): 148-149, 152.
- [9] 吴国华, 吴秦寒, 周晓栋. 一种基于小波变换的音频零水印算法 [J]. 机电工程, 2009, 26(9): 16-19.
- WU Guohua, WU Qinhan, ZHOU Xiaodong. An audio zero-watermarking algorithm based on DWT [J]. Mechanical & Electrical Engineering Magazine, 2009, 26(9): 16-19.
- [10] 王铭, 张玲华. 基于能量选择的 DCT 域音频数字水印算法 [J]. 计算机技术与发展, 2013, 23(2): 233-236.
- WANG Ming, ZHANG Linghua. An audio digital watermark algorithm in DCT domain based on energy selection [J]. Computer Technology and Development, 2013, 23(2): 233-236.
- [11] 蔡咏梅, 郭文强. 基于 DWT-SVD 的音频零水印算法 [J]. 计算机工程与设计, 2014, 35(1): 42-46.
- CAI Yongmei, GUO Wenqiang. Audio zero watermark algorithm based on DWT-SVD [J]. Computer Engineering and Design, 2014, 35(1): 42-46.
- [12] LALITHA N V, PRASAD P V, RAO S U. Performance analysis of DCT and DWT audio watermarking based on SVD [C]// 2016 International Conference on Circuit, Power and Computing Technologies (IC-CPCT). Piscataway, NJ, USA: IEEE, 2016: 1-5.
- [13] WANG M L, LIN H X, LEE M T. Robust audio watermarking based on MDCT coefficients [C]// 2012 Sixth International Conference on Genetic and Evolutionary Computing. Piscataway, NJ, USA: IEEE, 2012: 372-375.
- [14] ELSHAZLY A R, NASR M E, FUAD M M, et al. Synchronized double watermark audio watermarking scheme based on a transform domain for stereo signals [C]// 2016 Fourth International Japan-Egypt Conference on Electronics, Communications and Computers (JEC-ECC). Piscataway, NJ, USA: IEEE, 2016: 52-57.
- [15] SHI H, LI M C, GUO C, et al. A region-adaptive semi-fragile dual watermarking scheme [J]. Multimedia Tools and Applications, 2016, 75(1): 465-495.
- [16] WANG Q, HE M Q, DU M X, et al. Searchable encryption over feature-rich data [J]. IEEE Transactions on Dependable and Secure Computing, 2018, 15(3): 496-510.
- [17] ICVPR. 局部敏感哈希 (locality-sensitive hashing, LSH) 方法介绍 [EB/OL]. (2013-10-06) [2018-12-01]. <https://blog.csdn.net/icvpr/article/details/12342159>.
- [18] 吴瑾, 彭延国, 崔江涛. 基于局部敏感哈希的安全相似性查询方案 [J]. 密码学报, 2018, 5(2): 196-205.
- WU Jin, PENG Yanguo, CUI Jiangtao. Secure similarity search based on locality sensitive hashing [J]. Journal of Cryptologic Research, 2018, 5(2): 196-205.
- [19] 李琪, 廖鑫, 屈国庆, 等. 基于 Arnold 变换的数字图像自适应隐写算法 [J]. 通信学报, 2016, 37(6): 192-198.
- LI Qi, LIAO Xin, QU Guoqing, et al. Adaptive steganography algorithm in digital image based on Arnold transform [J]. Journal on Communications, 2016, 37(6): 192-198.
- [20] ALI Z, TALHA M. Innovative method for unsupervised voice activity detection and classification of audio segments [J]. IEEE Access, 2018, 6: 15494-15504.
- [21] 李乐, 王玉英, 李小霞. 一种改进的小波能量熵语音端点检测算法 [J]. 计算机工程, 2017, 43(5): 268-274.
- LI Le, WANG Yuying, LI Xiaoxia. An improved wavelet energy entropy algorithm for speech endpoint detection [J]. Computer Engineering, 2017, 43(5): 268-274.
- [22] MENG Y J, TENG X Y, LIU H R, et al. A screening scheme based on energy for speech key-frame [C]// 2017 IEEE 17th International Conference on Communication Technology (ICCT). Piscataway, NJ, USA: IEEE, 2017: 1639-1643.
- [23] JHO N S, CHANG K Y, HONG D, et al. Symmetric searchable encryption with efficient range query using multi-layered linked chains [J]. The Journal of Supercomputing, 2016, 72(11): 4233-4246.
- [24] 任克强, 李慧, 谢斌. 基于 DWT 和 SVD 的自适应数字音频零水印算法 [J]. 计算机工程与应用, 2014, 50(12): 87-90, 95.
- REN Keqiang, LI Hui, XIE Bin. Adaptive digital audio zero-watermarking algorithm based on DWT and SVD [J]. Computer Engineering and Applications, 2014, 50(12): 87-90, 95.

(编辑 陶晴)