

用于内容认证的半脆弱音频零水印算法

刘光玉*, 张雪英, 马朝阳

(太原理工大学 信息工程学院, 太原 030024)

(* 通信作者电子邮箱 bugaoni111@126.com)

摘要:提出了一种可用于版权和内容认证的半脆弱音频零水印算法,该算法提取载体音频的中低频分量构造零水印,确保了水印算法的不可感知性,并可实现盲检测。采用自适应的音频分帧方法,合理地分配了水印图像的像素点,从而提高了算法的篡改定位能力和对于常规攻击的鲁棒性。同时利用多级置乱技术消除水印图像的相关性,提高了算法的安全性以及对于常规攻击的鲁棒性。算法不但可进行完整性认证,还可以通过篡改评估准确定位篡改区域。实验结果表明,该算法对于常规攻击具有较好的鲁棒性,对恶意攻击还体现了很强的篡改定位能力。

关键词:零水印;半脆弱水印;内容认证;篡改定位;自适应分帧

中图分类号: TN918.91 **文献标志码:** A

Semi-fragile audio zero-watermarking algorithm for content authentication

LIU Guang-yu*, ZHANG Xue-ying, MA Zhao-yang

(College of Information Engineering, Taiyuan University of Technology, Taiyuan Shanxi 030024, China)

Abstract: This paper proposed a new semi-fragile audio zero-watermarking algorithm which can be used to authenticate the copyright and content of digital data. This algorithm has the following features: (1) it extracted the low frequency components of host audio to construct zero-watermarking, ensured the imperceptibility of watermarking algorithm, and achieved blind detection; (2) it distributed the pixels of watermarking images rationally by adopting an adaptive audio segmentation frame method, and improved the capability of tampering localization and robustness of regular attacks; (3) it used multilevel scrambling technology to eliminate the correlation of the watermarking images, improved its safety and the robustness toward regular attacks. Meanwhile, this algorithm can not only conduct the integrity authentication, but also locate the tampering area accurately by tampering assessment. The experimental result shows that this algorithm has good robustness toward regular attacks and strong capability of tampering localization toward malicious attacks.

Key words: zero-watermarking; semi-fragile watermarking; content authenticity; tampering location; adaptive frame

0 引言

目前,数字音频水印技术已广泛应用于版权认证、内容认证、隐蔽通信、拷贝控制、广播监控等多种领域。实现数字音频的内容认证,主要是依靠脆弱性水印。脆弱性水印可分为两种:完全脆弱水印和半脆弱水印。完全脆弱水印对音频的常规处理也很敏感,因此应用范围比较小;而半脆弱水印对常规攻击体现了较好的鲁棒性,还能区别恶意篡改,并对篡改进行定位,因此,具有更重要的研究价值。

本文提出一种半脆弱音频零水印算法,它对于常规攻击具有较好的鲁棒性,对恶意攻击还体现了很强的篡改定位能力。算法选择音频的中低频分量构造半脆弱零水印:首先,将水印图像进行分块、多级置乱后,重构为一个一维序列作为水印信息,以消除水印图像的相关性,提高算法的安全性和鲁棒性;同时,根据原始音频的能量,对音频进行自适应的分帧,以提高算法的篡改定位能力和对常规攻击的鲁棒性;然后,对每帧信号进行三级小波分解,提取小波中低频系数构造一个二值序列,并将此二值序列与水印信息进行异或运算,生成零水印。水印检测时,采用相同的方法,将生成的二值序列与零水印进行异或运算,提取水印信息,重构水印图像;最后,通过篡改评估定位篡改区域。由于采用零水印技术,整个过程没有

对原始音频进行任何修改,保证了算法的透明性,并能够实现盲检测。

1 理论基础

1.1 零水印技术

在数字水印系统中,透明性和鲁棒性始终是一对矛盾因素。对于用于版权保护和内容认证的音频水印来说,透明性是前提。因此,要在保证水印不可感知性的前提下,保证其具有较好的鲁棒性和抗攻击性。

零水印是一种典型的数字水印系统,它起源于图像水印,后逐渐在音频水印中占有重要地位。零水印不仅很好地解决了数字水印的不可感知性和鲁棒性之间的矛盾,而且克服了准可逆水印系统中存在的安全漏洞。零水印技术与常规的水印算法的区别在于:它是一种非嵌入式的数字水印技术,即构造过程没有向载体信息中嵌入水印,而是提取载体音频的重要特征来构造“零水印”。

1.2 自适应分帧

目前,所有用于内容完整性认证的音频水印技术,几乎都是通过原始音频段与二值图像像素点间的一一对应关系来实现篡改定位的,即每一帧音频对应一个水印图像像素点。也就是说,水印图像的大小限制了对原始音频分帧的总帧数。

收稿日期:2011-10-28;修回日期:2011-12-03。

作者简介: 刘光玉(1984-),男,山西太原人,硕士研究生,主要研究方向:数字音频水印; 张雪英(1964-),女,河北石家庄人,教授,博士生导师,主要研究方向:语音识别、数字音频水印、语音编码; 马朝阳(1980-),男,山西运城人,博士研究生,主要研究方向:数字音频水印。

那么,在音频总帧数一定的前提下(即水印图像大小不变),如何最有效地对原始音频分帧就非常值得研究了。而目前的水印算法为保证水印图像覆盖整个音频,普遍采用平均分帧的方法,即每帧音频具有相等的长度。例如,对于 64×64 的二值水印图像,在预处理时就对应地把原始音频平均分为 64×64 帧。显然,这样的处理不能最合理地分配水印图像的像素点。一个比较极端的例子是:假设原始音频中有大段的空白段,那分配给这段空白的音频帧就被“浪费”了。

因此,本文提出了一个根据原始音频能量来自适应分帧的方法。简单地说,就是对能量较大的音频段给予更多的帧数,而对于能量较小的音频段给予较少的帧数,使得每帧信号具有相等的能量大小。以 64×64 的水印图像为例(总帧数为 4096),首先,计算原始音频的总能量和每帧音频段的平均能量。然后,对音频信号能量逐一累加,每当累加值大于或等于平均能量就认为此段音频满足一次分帧条件,则记下此时的样点坐标,并把累加值重新赋初值再进行累加。(由于每次满足分帧条件时的累加值很难准确地等于平均能量值,所以如果每次都记下超出后的样点坐标,那就会每帧多取一个样点。这样当分帧全部完成时,最后一帧数据会少 4095 个样点,若音频很短则会无法完成分帧;而如果每次都取超出时前一点的坐标,则最后一帧数据会因为多了 4095 个样点而不准确。因此在满足分帧条件并记下坐标后,需进行一次判定:对于偶数帧,将累加值清零;对于奇数帧,则将累加值赋值为当前样点能量。这样,当分帧全部完成后,尽管奇数帧多一个样点,偶数帧少一个样点,但不会影响整体的分帧过程。直到达到总帧数 4096 帧,停止累加,并将这 4096 个坐标点作为一组密钥。在水印构造和提取的算法中,则根据此密钥,对音频进行分帧处理。这样,就使得每帧音频信号具有相等的能量,从而不仅让水印图像完整覆盖了整个音频,而且很好地利用了各像素点和音频段的一一对应关系,提高了算法的篡改定位能力。

2 算法描述

2.1 水印图像预处理

原始水印图像为一幅 $N \times N$ 的有意义二值图像,记为 $V = \{v(i, j), 1 \leq i \leq N, 1 \leq j \leq N\}$,其中 $v(i, j) \in \{0, 1\}$ 表示水印图像的第 i 行,第 j 列的像素点灰度值。

步骤 1 将 V 分成四个子块,记为 $V_n = \{v(i, j), 1 \leq i \leq N/2, 1 \leq j \leq N/2\}$,其中 $n \in \{1, 2, 3, 4\}$;

步骤 2 对每个子块 V_n 进行 Arnold 置乱操作,置乱次数作为密钥 K_3 ;

步骤 3 将每个子块降维重构为一维数组 $K_{2n}(i), i = 1, 2, \dots, \frac{N}{2} \times \frac{N}{2}, n \in \{1, 2, 3, 4\}$,再将得到的 4 个 K_{2n} 合并为一个一维数组,记为 $K_2(i), i = 1, 2, \dots, N \times N$ 。

2.2 自适应分帧

步骤 1 设原始音频信号为 $x(n)$,其长度为 L ,原始水印图像为一幅 $N \times N$ 的有意义二值图像,总帧数 $N \times N$ 作为密钥 K_1 。首先对 $x(n)$ 求绝对值,并把新的序列记为 $|x(n)|$;然后求出每帧音频的平均能量,记为 \bar{Q} ,其中:

$$\bar{Q} = \frac{\sum_{i=1}^L |x(i)|}{N \times N} \quad (1)$$

步骤 2 对序列 $|x(n)|$ 中的元素逐一求和,记为 $Q, Q = Q + |x(i)|, i = 1, 2, \dots, L$;当 $Q \geq \bar{Q}$ 时,认为满足一次分帧条件,则令 $K_4(j) = i, j = 1, 2, \dots, N \times N$,同时令:

$$Q = \begin{cases} |x(i)|, & j \text{ 为奇数} \\ 0, & j \text{ 为偶数} \end{cases} \quad (2)$$

步骤 3 把 Q 作为初值,令 $j = j + 1$,重复步骤 2,直到 $j > N \times N$ 时结束;并令 $K_4(1) = 1, K_4(N \times N + 1) = L$;同时把序列 $K_4(j), j = 1, 2, \dots, N \times N + 1$ 作为密钥发送。

2.3 水印的构造

图 1 概括嵌入过程的流程,虚线上面是对原始音频的处理,虚线下面是水印图像的预处理。

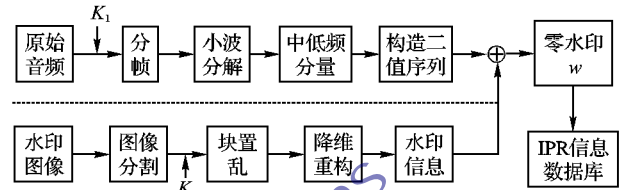


图1 嵌入过程流程

步骤 1 根据密钥 K_1 和 $K_4(j), j = 1, 2, \dots, N \times N + 1$ 将原始音频 $x(n)$ 分为 K_1 个子序列 $x_1(n), x_2(n), \dots, x_{K_1}(n)$, 每个子序列作为一帧信号,则第 i 帧信号可记为:

$$x_i(n) = \{x[K_4(i)], x[K_4(i) + 1], \dots, x[K_4(i + 1) - 1], x[K_4(i + 1)]\}; i = 1, 2, \dots, N \times N$$

步骤 2 对第 i 帧信号 ($i = 1, 2, \dots, K_1$) 进行三级小波分解,小波基函数选用“db4”,得到 m 个小波中低频系数,记为 $c_i(j), j = 1, 2, \dots, m$ 。

步骤 3 对每帧得到的小波系数求平均值,记为 $\bar{c}(i), i = 1, 2, \dots, K_1$,其中:

$$\bar{c}(i) = \frac{\sum_{j=1}^m c_i(j)}{m}; i = 1, 2, \dots, K_1 \quad (3)$$

令 $cp = (\sum_{i=1}^{K_1} \bar{c}(i)) / K_1$,根据 $\bar{c}(i), i = 1, 2, \dots, K_1$ 与 cp 的关系产生一个二值序列,记为 $y(i), i = 1, 2, \dots, K_1$,其中:

$$y(i) = \begin{cases} 1, & \bar{c}(i) \geq cp \\ 0, & \bar{c}(i) < cp \end{cases} \quad (4)$$

其中 $i = 1, 2, \dots, K_1$ 。

步骤 4 将水印图像预处理后得到的一维数组 $K_2(i), i = 1, 2, \dots, K_1$,与产生的二值序列 $y(i), i = 1, 2, \dots, K_1$ 进行异或运算,得到零水印,记为 $w(i), i = 1, 2, \dots, K_1$,其中:

$$w(i) = y(i) \oplus K_2(i); i = 1, 2, \dots, K_1 \quad (5)$$

最后,将得到的零水印提交 IPR 信息数据库进行注册。

2.4 水印的提取

图 2 概括了水印提取过程的流程,虚线上面是待测音频的处理,虚线下面是水印图像的重构和检测过程。具体步骤如下:

步骤 1 输入密钥 K_1 和 $K_4(j), j = 1, 2, \dots, N \times N + 1$,将待测音频 $x'(n)$ 分为 K_1 个子序列 $x'_1(n), x'_2(n), \dots, x'_{K_1}(n)$,每个子序列作为一帧信号,则第 i 帧信号可记为:

$$x'_i(n) = \{x'[K_4(i)], x'[K_4(i) + 1], \dots, x'[K_4(i + 1) - 1], x'[K_4(i + 1)]\}; i = 1, 2, \dots, N \times N$$

步骤 2 对第 i 帧信号 ($i = 1, 2, \dots, K_1$) 进行三级小波分解,小波基函数选用“db4”,得到 m' 个小波中低频系数,记为

$c'_i(j), j = 1, 2, \dots, m'$;

步骤3 对每帧得到的小波系数求平均值,记为 $\bar{c}'(i)$,
 $i = 1, 2, \dots, K_1$,其中:

$$\bar{c}'(i) = \frac{\sum_{j=1}^{m'} c'_i(j)}{m'}; i = 1, 2, \dots, K_1 \quad (6)$$

令 $cp' = \left(\sum_{i=1}^{K_1} \bar{c}'(i) \right) / K_1$,根据 $\bar{c}'(i), i = 1, 2, \dots, K_1$ 与 cp' 的关系产生一个二值序列,记为 $y'(i), i = 1, 2, \dots, K_1$,其中:

$$y'(i) = \begin{cases} 1, & \bar{c}'(i) \geq cp' \\ 0, & \bar{c}'(i) < cp' \end{cases}; i = 1, 2, \dots, K_1 \quad (7)$$

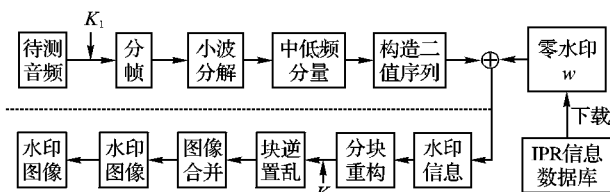


图2 提取过程流程

步骤4 下载并输入零水印 $w(i), i = 1, 2, \dots, K_1$,对求得的二值序列 $y'(i), i = 1, 2, \dots, K_1$ 和 $w(i), i = 1, 2, \dots, K_1$ 进行异或运算,获得提取出的水印,记为 $w'(i), i = 1, 2, \dots, K_1$,其中:

$$w'(i) = y'(i) \oplus w(i); i = 1, 2, \dots, K_1 \quad (8)$$

步骤5 将提取的水印序列 $w'(i), i = 1, 2, \dots, K_1$ 分成4段,记为 $w_n'(i), i = 1, 2, \dots, \frac{N}{2} \times \frac{N}{2}, n \in \{1, 2, 3, 4\}$,将每个 w_n' 重构为 $\frac{N}{2} \times \frac{N}{2}$ 的矩阵 $V_n' = \{v'(i, j), 1 \leq i, j \leq \frac{N}{2}\}, n \in \{1, 2, 3, 4\}$;

步骤6 输入密钥 K_3 ,将 V_n' 进行Arnold逆置乱,并将逆置乱后的矩阵重构为 $N \times N$ 的矩阵 $V' = \{v'(i, j), 1 \leq i, j \leq N\}$,即得到提取的水印图像。

3 仿真实验结果和性能分析

水音 印频

图3 水印图像

本实验采用 Matlab7.8 作为仿真软件,选取采样频率为 44.1 kHz, 16 bits 作为音频信号, 64×64 的二值图像作为水印图像,取 $K_3 = 10$ 。如图3所示。

实验将原水印图像与提取的水印图像通过相似度(Normalized Correlation Coefficient, NC)检测器进行相似度检测,其检测公式如下:

$$NC(W, W') = \frac{\sum_i w(i)w'(i)}{\sqrt{\sum_i w^2(i)} \sqrt{\sum_i w'^2(i)}} \quad (9)$$

其中: W 为原始水印, W' 为提取出的水印。

同时,计算出水印篡改评估函数(Tamper Assessment Function, TAF),TAF定义为:

$$TAF(w, w') = \frac{1}{N} \sum_{i=1}^N w(i) \oplus w'(i) \quad (10)$$

其中: w 表示原始水印图像, w' 表示提取的水印图像。


TAF表示的是水印的篡改程度,若TAF值等于0,则没有发生篡改,否则发生篡改;TAF值越接近于1,说明篡改程度越高。

3.1 鲁棒性测试

为了说明半脆弱水印本身对常规信号处理具有一定的攻击能力,在篡改没有发生的时候,分别对原始语音进行了如下处理:1)加入均值为0,方差分别为0.01和0.02的高斯白噪声;2)用6阶截止频率为15 kHz的巴特沃兹滤波器滤波;3)32 bits和8 bits的重量化;4)128 Kbps和64 Kbps的MP3压缩等常规处理。

表1为待检测音频在遭到上述攻击后提取出来的水印图像、未经逆置乱恢复的水印图像以及归一化相关系数(NC)和误码率(Bit Error Rate, BER)。

表1 常规攻击下半脆弱水印的检测结果

算法	文献[1]算法		传统分帧方法		本文算法		本文提取的水印信息	
	NC	BER	NC	BER	NC	BER	提取出的水印图像	未经逆置乱的水印图像
未受攻击	1.0000	0.0000	1.0000	0.0000	1.0000	0.0000	水音印频	
加噪(0,0.01)	0.9990	0.0014	0.9828	0.0168	0.9954	0.0056	水音印频	
加噪(0,0.02)	0.9206	0.0752	0.9656	0.0330	0.9892	0.0127	水音印频	
滤波(15 kHz)	0.8571	0.1348	0.9263	0.0691	0.9910	0.0095	水音印频	
重量化(16→8→16 bits)	0.9885	0.0088	0.9755	0.0244	0.9966	0.0046	水音印频	
重量化(16→32→16 bits)	1.0000	0.0000	0.9973	0.0034	0.9997	0.0007	水音印频	
MP3 压缩(128 Kbps)	1.0000	0.0000	0.9928	0.0081	0.9978	0.0024	水音印频	
MP3 压缩(64 Kbps)	0.9989	0.0001	0.9802	0.0186	0.9935	0.0061	水音印频	

实验数据证明:以上几种典型的常规攻击并不会对水印信息造成太大的改变,也就是说,本文构造的半脆弱水印对于常规攻击体现了较好的鲁棒性。另外,还对其他一些常规攻击(如幅度放大、缩小等)的抗攻击性能进行了实验,结果同样有所改进。

从水印图像来看:音频遭到常规攻击后,用该算法提取的水印图像依然清晰可见,说明一定容许范围内的常规攻击,并不影响音频水印的鉴定;同时,未经逆置乱恢复的水印图像,在遭到常规攻击后,像素点分布均匀,图像未发生整块的缺失,也证明了算法对于常规攻击比较稳定。以上就证明了该算法可以实现音频的版权认证。

另外,从与文献[1]实验结果的对比中可以看出,在对其他攻击鲁棒性差别很小的情况下,本算法对于滤波和加噪两种攻击,体现了更好的鲁棒性,尤其是在噪声比较大或者联合攻击的时候,就更能体现本算法的优越性。

本文还做了另一组仅改变分帧方法的对比实验,就是在其他算法不改变的情况下,采用传统的方法对音频进行平均分帧处理,而不使用自适应分帧的方法。从表1中数据可以看出,采用自适应分帧处理的算法,对于所有的常规攻击,其鲁棒性都有所改善。

3.2 篡改检测与定位

下面,对原始音频做最常见的两种恶意攻击(剪切和替换),并通过 TAF 函数来检验本算法的篡改定位能力。本文实验设置 TAF 阈值为 0.2,即当 $TAF > 0.2$ 时,则认为此段音频发生了篡改,并返回可能发生篡改的采样点范围。

1) 剪切攻击。

对原始音频进行 1/20 长度(20 000 至 23 000 采样点)的剪切,生成被恶意篡改的待检测音频,然后从中提取水印图像,所得结果如图 4 所示。

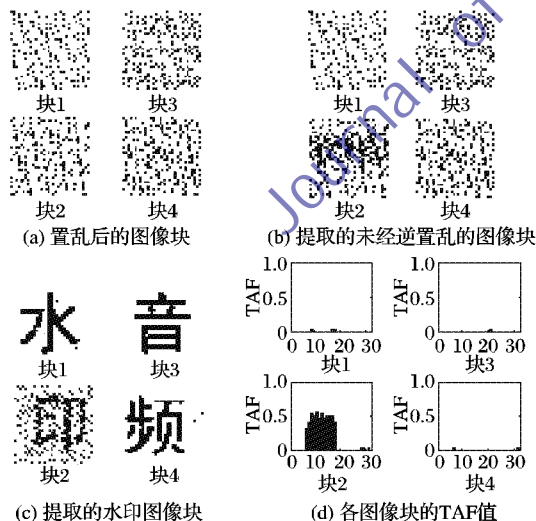


图4 剪切音频 1/20 的实验结果

从图 4(c) 可以看到,水印图像的第二块发生了明显的变化,而其他几块无明显变化,因此可以大致推断音频的第二大段遭到了恶意攻击;再对比观察图(a)与(b)可以看出,与常规攻击不同,篡改导致的水印图像像素点分布不均匀,图中第二图像块的中部像素点明显改变;图 4(d) 则进一步精确定位了发生恶意攻击的位置,可以看到,其余几个图像块的 TAF 值无明显变化,而第二块部分 TAF 值都超过了 0.2,由此可以

确定,音频的第二大段发生了篡改。同时,程序返回篡改范围为 19 886 至 23 053 采样点。

2) 替换攻击。

用另外一个采样率和量化精度与本文相同的音频段来代替原始音频中 1/20 长度(20 000 至 23 000 采样点),生成被替换攻击的待检测音频,然后从中提取水印图像,所得结果如图 5 所示。

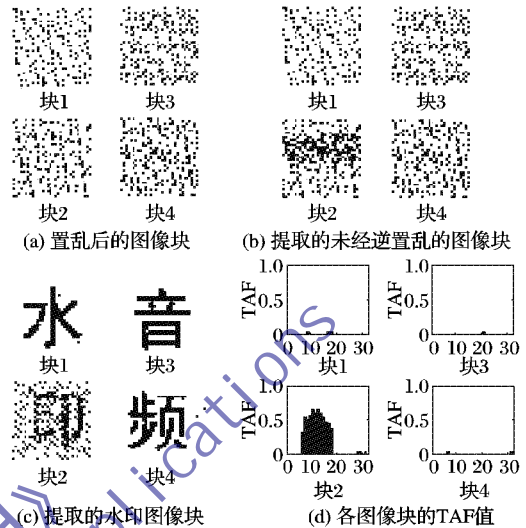


图5 替换音频 1/20 的实验结果

与剪切攻击类似,从图 5 的实验结果依然可以逐层定位恶意攻击发生的位置。上述结果验证了系统对恶意攻击高效的定位能力。

3) 联合攻击。

下面检测算法在常规攻击和恶意攻击联合攻击下的篡改定位能力:首先用 5 阶截止频率为 15 kHz 的巴特沃兹滤波器对原始音频滤波;再加入均值为 0,方差为 0.02 的高斯白噪声;然后对音频进行 1/20 长度(23 000 至 26 000 采样点)的剪切,同时,用另外一个音频段来替换音频中 1/20 长度(33 000 至 36 000 采样点),生成被恶意篡改的待检测音频,然后从中提取水印图像,所得结果如图 6 所示。

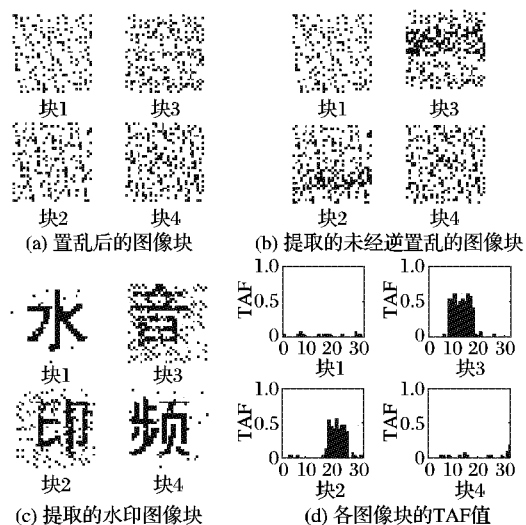


图6 联合攻击实验结果

从图 6 的实验结果可以看出(程序返回篡改范围为 [23 058, 26 053] 和 [32 957, 35 940] 区间的采样点),在滤波、加噪、剪切和替换的联合攻击下,算法依然体现了较为精确的

篡改定位能力。但是,从图 6(d)来看,单从水印图像和 TAF 值,仅能定位篡改发生的位置,仍无法区分恶意攻击的类型。不过,可以通过对比遭到篡改音频段的波形,来进一步区分此段语音究竟是遭到了剪切,还是替换攻击。

定位了篡改位置后,可以进一步提取出篡改发生段音频的波形,如图 7 所示。

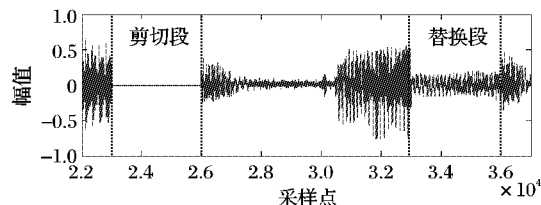


图 7 篡改发生段待测音频波形

图中两虚线间的音频段为发生篡改的音频段,对比两个篡改段可以看出,左边音频段的篡改比较彻底,幅度变成了零,可以推断该段音频遭到了剪切攻击;而右边的篡改段依然有一定的幅度,很可能是被替换成了另一段音频,可以推断该段音频遭到了替换攻击。由此,就能进一步对两种恶意攻击进行区分。

4 结语

本文提出一种可用于内容认证的半脆弱音频零水印算法,将自适应思想和零水印技术结合起来,采用图像分块、Arnold 变换和小波分解等方法完成了水印图像的嵌入和提取,并将分割的图像块和自适应分帧处理后的音频段一一对应起来,使得算法效率更高,篡改定位更加准确。其特点是在不改变载体音频的前提下,完成对载体音频的完整性认证,并准确定位篡改区域。实验结果说明,本算法不但对常规攻击具有较好的鲁棒性,而且对恶意攻击还具有较好的篡改定位

能力,同时计算简单,易于实现,具有很高的应用价值。

参考文献:

- [1] 杨晋霞, 马朝阳, 张雪英. 基于小波包分析的数字音频双水印算法[J]. 计算机应用, 2010, 30(5): 1218 - 1220.
- [2] WU SHAO-QUAN, HUANG JI-WU, MEMBER S. Efficiently self-synchronized audio watermarking for assured audio data transmission [J]. IEEE Transactions on Broadcasting, 2005, 51(1): 69 - 76.
- [3] MENDELZON A O, RIZZOLO F, VAISMAN A. Indexing temporal XML documents[C]// VLDB'04: Proceedings of the Thirtieth International Conference on Very Large Data Bases. [S. l.]: VLDB Endowment, 2004: 216 - 227.
- [4] MARTIN S, PETITCOLAS F A P. Stirmark benchmark: Audio watermarking attacks[EB/OL]. [2011 - 06 - 01]. http://private.sit.fhg.de/~steineba/publikationen-Dateien/itcc01_stirmark.pdf.
- [5] 温泉, 孙铁锋, 王树勋. 零水印的概念和应用[J]. 电子学报, 2003, 31(2): 214 - 216.
- [6] 张小华, 孟红云, 刘芳, 等. 一类有效的脆弱型数字水印技术[J]. 电子学报, 2004, 32(1): 114 - 117.
- [7] 张兵路, 姜建国, 冯复科, 等. 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 - 152.
- [8] 全笑梅, 张鸿宾. 用于篡改检测及认证的脆弱音频水印算法[J]. 电子与信息学报, 2005, 27(8): 1187 - 1191.
- [9] 王向阳, 祁薇. 用于版权保护与内容认证的半脆弱音频水印算法[J]. 自动化学报, 2007, 33(9): 937 - 940.
- [10] 桑军, 张之刚, 向宏. 基于人工神经网络的半脆弱零水印技术[J]. 计算机工程与应用, 2009, 45(16): 93 - 95.
- [11] 廖婉名, 张玉贤, 李东晓, 等. 基于小波变换的脆弱 - 鲁棒双重音频水印[J]. 浙江大学学报: 工学版, 2009, 43(4): 722 - 726.
- [12] 叶天语, 钮心忻, 杨义先. 多功能双水印算法[J]. 电子与信息学报, 2009, 31(3): 546 - 551.

(上接第 970 页)

完整性和身份真实性的 RFID 系统认证协议的安全需求。

5 结语

随着电子商务和物联网的发展,RFID 技术被广泛应用,人们越来越多地关注安全和隐私问题。现有的认证协议中,大多存在某些安全隐患或者不符合 EPC Gen2 标准的要求,无法成为实际可用的 RFID 系统安全机制。本文在对以往协议分析研究的基础上,总结以往协议存在漏洞的基本原因,提出新的认证协议,经安全性分析,新提出的协议符合 EPC Gen2 标准,并且能够满足 RFID 协议的各种安全需求。

参考文献:

- [1] SARMA S E, WEIS S A, ENGELS D W. RFID systems and security and privacy implications[C]// Proceedings of CHES'02 Revised Papers from the 4th International Workshop on Cryptographic Hardware and Embedded Systems. London: Springer-Verlag, 2003: 454 - 469.
- [2] SARMA S E, WEIS S A, ENGELS D W. Radio-frequency identification: Secure risks and challenges[J]. RSA Laboratories CryptoBytes, 2003, 6(1): 2 - 9.
- [3] WEIS S A, SARMA S E, RIVEST R L. Security and privacy aspects of low-cost radio frequency identification systems[C]// Security in Pervasive Computing, LNCS 2802. Berlin: Springer-Verlag, 2004: 201 - 212.
- [4] EPCglobal. The EPCglobal architecture framework[S/OL]. [2011

- 11 - 06]. http://www.epcglobalinc.org/standards/architecture/architecture_1_3-framework-20090319.pdf.

- [5] BURROWS M, ABADI M, NEEDHAM R. A logic of authentication [J]. ACM Transactions in Computer Systems, 1990, 9(1): 18 - 36.
- [6] PERIS-LOPEZ P, HERNANDEZ-CASTRO J C, TAPIADOR J E, et al. Weaknesses in two recent lightweight RFID authentication protocols[C]// Inscrypt'09: Proceedings of the 5th International Conference on Information Security and Cryptology. Berlin: Springer-Verlag, 2009: 383 - 392.
- [7] CHEN C-L, DENG Y-Y. Conformation of EPC class 1 and generation 2 standards RFID system with mutual authentication and privacy protection[J]. Engineering Applications of Artificial Intelligence, 2009, 22(8): 1284 - 1291.
- [8] BURMESTER M, de MEDEIROS B, MUNILLA J, et al. Secure EPC Gen2 compliant radio frequency identification[C]// ADHOC-NOW'09: Proceedings of the 8th International Conference on Ad-Hoc, Mobile and Wireless Networks. Berlin: Springer-Verlag, 2009: 227 - 240.
- [9] PIRAMUTHU S. RFID mutual authentication protocols[J]. Decision Support Systems, 2011, 50(2): 387 - 393.
- [10] 邓森磊, 黄照鹤, 鲁志波. EPC Gen2 标准下安全的 RFID 认证协议[J]. 计算机科学, 2010, 37(7): 115 - 117.
- [11] MITRA M. Privacy for RFID systems to prevent tracking and cloning [J]. International Journal of Computer Science and Network Security, 2008, 8(1): 1 - 5.