一种基于混沌和小波变换的大容量音频信息隐藏算法

谭 良[1,2],吴 波[1],刘 震[3],周明天[3]
(1.四川省可视化计算与虚拟现实重点实验室,四川师范大学计算机学院,四川成都 610068;
2.中国科学院计算技术研究所,北京 100080;3.电子科技大学计算机科学与工程学院,四川成都 610054)

摘 要: 音频信息隐藏的主要原理是利用人耳听觉系统的某些特性,将秘密信息隐藏到普通的音频数据流中以达到隐蔽通信的目的.提出了一种基于混沌和小波变换的大容量音频隐藏算法.该算法首先利用混沌序列良好的伪随机特性对秘密信息进行置乱加密预处理;然后利用人耳对音频的采样倒置并不敏感,可以通过倒置的方法改变载体信息小波系数正负极性的特点,将加密后的秘密信息通过一对一地变更小波域高低频部分对应位正负极性的方法隐藏到载体信息中.实验结果表明,该算法不仅具有良好的不可感知性和鲁棒性,能够抵御噪声攻击、重采样攻击、重量化攻击以及 MP3 压缩攻击等,而且信息隐藏容量大,可实现盲检测.

关键词: 信息隐藏; 混沌; 小波变换; 采用点倒置
中图分类号: TP311 **文献标识码:** A **文章编号:** 0372-2112 (2010) 08-1812-07

An Audio Information Hiding Algorithm with High-Capacity Which Based on Chaotic and Wavelet Transform

TAN Liang[1,2], WU Bo[1], LIU Zhen[3], ZHOU Ming-tian[3]
(1. *Key Lab of Visualization in Scientific Computing and Virtual Reality of Sichuan College of Computer, Sichuan Normal University, Chengdu, Sichuan* 610068, *China*; 2. *Institute of Computing Technology, Chinese Academy of Sciences, Beijing* 100080, *China*; 3. *School of Computer Science and Engineering, University of Electronic Seience and Technology of China, Chengdu, Sichuan* 610054, *China*)

Abstract: Audio information hiding hides the secret message into the audio data flows by some characteristics of human auditory system. An audio information hiding algorithm with high-capacity which based on chaotic and wavelet transform is proposed, which, scrambles the secret message by chaotic sequences, and then one-to-one hides those into the high and low frequency of the wavelet field of the cover message by changing the cover message's wavelet domain coefficient's polarity based on the features that audio sample dots inversion has little influence on the human hearing. Experimental results show that this algorithm not only has good imperceptibility and is robust against different kinds of attacks, such as noise adding, re-quantizing, re-sampling, MP3 compression, and so on, but also has high-capacity, and can realize the blind detection.

Key words: information hiding; chaotic; wavelet transform; sample dots inversion

1 引言

音频信息隐藏是信息隐藏的一个重要分支,其主要原理是利用人耳听觉系统的某些特性,将秘密信息隐藏到普通的音频数据流中以达到隐蔽通信的目的.音频信息隐藏作为一种有效的信息安全手段能够掩盖秘密通信的存在,避免攻击者对通信内容进行非法监控和破坏,是当前数字音频处理研究的重要内容.

近年来,国内外音频信息隐藏领域的研究得到了迅速发展,出现较多相关的文献和著述,从各个不同的角度提出了多种隐藏算法.总的来说,这些算法大致可以分为时(空)域算法和变换(频)域算法两类.时(空)域方法主要是用秘密信息替换载体信息中的冗余部分.这种方法较为简单,但其鲁棒性较差,对载体较小的扰动,如有损压缩,都有可能导致秘密信息的丢失.时(空)域算法中最具代表性的有:最不重要位算法[1,2]、回声隐藏算法[3,4]、扩频算法[5,6]、以及相位编码算法[7,8].变换(频)域算法利用人类感知系统对不同频率的敏感性,

收稿日期:2009-06-23;修回日期:2009-10-05
基金项目:国家自然科学基金面上项目(No.60970113);青年基金(No.60903073);四川省科技厅项目(No.2008JY0105-2);四川省教育厅项目(No.07ZA091)

把秘密信息隐藏到载体信息的一个变换空间(如频域)中不可感知性和鲁棒性较高的区域.常用的变换域算法有:基于离散傅立叶变换(DFT)[9]、基于离散余弦变化(DCT)[10]和基于离散小波变换(DWT)[11]等.另外,也有一些文献基于听觉掩蔽模型的隐藏方法将信息嵌入方法与心理声学模型算法紧密结合起来,确保算法的透明性[12~14].

通过对当前各种主流音频隐藏算法的分析,我们发现不管是时(空)域算法、变换(频)域算法还是基于听觉掩蔽模型的隐藏方法,多数的算法研究都将主要关注点放在提高音频隐藏的不可感知性和鲁棒性方面,相比之下,在以下两个方面做得不足:首先多数音频隐藏算法对秘密信息的预处理不够充分.部分算法或将音频秘密信息进行了简单的置换,或将音频秘密信息进行简单的加密.由于一般的音频秘密信息均具有的自相关和互相关特性,只进行简单的置换或加密不能很好隐藏秘密信息的自相关和互相关特征.因此,如果不进行预处理或者预处理不充分,很容易被攻击者利用并进行攻击;其次,绝大多数音频隐藏算法均不能兼顾隐藏容量、鲁棒性和透明性.例如,LSB 算法隐藏容量大,但鲁棒性、透明性差; 相位隐藏法、回声隐藏法鲁棒性、透明性好但容量低,扩频方法鲁棒性好,但透明性和容量不能兼顾.DFT、DCT 和 DWT 算法鲁棒性和透明性不能兼顾,且隐藏容量有限等等.

因此,针对以上存在的问题,在如何对秘密信息进行预处理以及如何设计一种隐藏容量大、透明性和鲁棒性好的音频隐藏算法方面做出了一些研究和探索,具有非常重要的现实意义.本文提出了一种基于混沌和小波变换的大容量音频隐藏算法.该算法首先利用混沌良好的伪随机特性对秘密信息进行置乱加密预处理.然后,利用人耳对音频的采样倒置并不敏感,可以通过倒置的方法改变载体信息小波系数正负极性的特点,将加密后的秘密信息通过修改小波系数正负极性的方法隐藏到载体信息的小波域.实验结果表明,该算法不仅具有良好的不可感知性和鲁棒性,能够抵御噪声攻击、重采样攻击、重量化攻击以及 MP3 压缩攻击等,而且信息隐藏容量大,可实现盲检测.

2　基于混沌和小波变换的大容量音频信息隐藏算法

2.1　基于混沌置乱的秘密信息预处理

目前,置乱技术很多,且大多用在数字图像加密上,如:Arnold 变换、幻方变换、分形 Hilbert 曲线、Tangram 算法、IFS 模型、Conway 游戏、Gray 码变换、广义 Gray 码变换等方法[15].这些算法各有优点和缺点,综合表现为置乱速度与安全性不能很好地兼顾,这是由于图像、音频和视频之类的多媒体数据均包含大量冗余信息,对这些包含大量冗余信息的内容进行置换处理需要消耗很大的资源,而且不能满足实时性的要求.在实际应用中,针对图像、音频和视频等多媒体数据信息量大的特点,目前常用混沌置乱和混沌序列密码的加密处理方法进行预处理.本算法将对音频秘密信息采用基于混沌序列的二次置乱预处理.首先通过分组有效地降低了生成伪随机序列的长度,然后将原音频信号经过两次置乱,可获得较好的随机特性,其具体方式和步骤如下:

(1)分组秘密信息:设秘密信息为 S,长度为 l_S.将 S 分为 l 组,每组长度为 l,其中 l_S 和 l 满足下列关系:$l^2 \leqslant l_S < (l+1)^2$.这样我们就将 S 分成了两个部分 S_e 和 S_r,其中 S_e 的长度为 l^2,是需要置乱的部分;S_r 是 S 长度超出 l^2 的部分(根据定义其长度 $l_r < l$),我们对其予以保留,不进行置乱处理.

(2)生成混沌排列:文献[16]通过使用统计检验和 E Cesato 检验两种方法对 Logistic 混沌序列进行随机性分析发现,针对具有以下形式的 Logistic 系统:

$$x_{n+1} = f(x_n) = 1 - \mu x_n^2 \tag{1}$$

在初值 $x_0 = 7$,参数 $\mu \in (1.99, 2]$时将产生具有最佳随机性的混沌序列.因此我们从上述形式的混沌系统中选取初值 $x_0 = 7$、$\mu = 1.997$ 为密钥来产生长度为 l 的混沌伪随机序列,设生成的序列为 $C = \{C_k \mid k = 1,2,3\cdots l\}$.其分布如图 1.

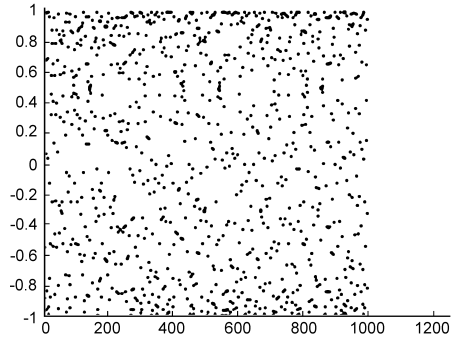


图1　长度l=1000时的混沌序列样本点分布

(3)二次置乱:设需要得到的伪随机排列为 $C' = \{C'_k \mid k = 1,2,3\cdots l\}$,则 $C'_k = \mathrm{mod}(\lfloor C_k * N \rfloor, l)$(其中 $k = 1,2,3,\cdots,l$,N 一般取 10 的乘幂).若计算得到的 C'_k 的当前值与之前某一位有重复,则将该位的数据加 1 后再继续与 l 做模运算,依理递归,最后得到一个长度为 l 的伪随机排列 C'.图 2 为原始秘密信息和二次置乱加密后的密秘信号的对比.

2.2　秘密信息的隐藏

将秘密信息隐藏到音频信号中时,通常要利用人耳听觉系统的某些特性.本算法将利用人耳听觉系统对音频的采样倒置并不敏感的特性,通过倒置的方法

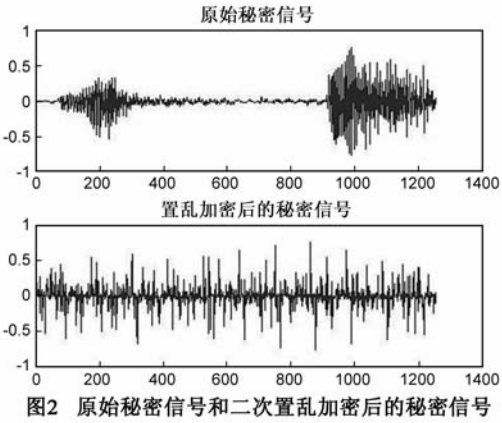


图2 原始秘密信号和二次置乱加密后的秘密信号

改变载波信号小波系数正负极性,从而达到隐藏秘密信息的目的.因此,在研究隐藏算法之前,我们首先对倒置的特性作进一步分析.

2.2.1 采样倒置分析

通过大量的样本实验发现,在小波域采用倒置系数的方法对音频信号进行处理时,其对载体音质的影响主要和下面几点有关:

采样点幅值:选取了一定数量的具有代表性的音频信号样本做一级小波分解,设置两个阈值 α 和 β(其中 $\alpha \leqslant \beta$,称 α 为低倒阈值、β 为高倒阈值),分别在时域中对每个样本的低频和高频部分做测试.测试方法如下:设所有 m 个正采样幅值的均值为 $\bar{P}_s$,n 个负采样幅值的均值为 $\bar{P}_n$,其中

$$\begin{cases} \bar{P}_s = \dfrac{1}{m}\sum_{i=1}^{m} p(i) \\ \bar{P}_n = \dfrac{1}{n}\sum_{i=1}^{n} |p(i)| \end{cases} \tag{2}$$

将 α 和 β 的初值在幅值为正数的部分为设为 $(\bar{P}_s + \bar{P}_n)/2$,幅值为负数设为 $-(\bar{P}_s + \bar{P}_n)/2$,取 $\Delta\varphi$ 为 α 和 β 的一个衰变步长,每次测试时在信号的高频或低频部分分别将系数幅值小于等于 α 和大于等于 β 的采样点倒置,然后对信号进行小波重构,比较重构信号和原信号在音质效果上的差异,每进行完一次,就将 α 的值向 0 方向衰减 $\Delta\varphi$,β 向反方向增加 $\Delta\varphi$.通过观察发现,在阈值衰变的初期,无论是在信号的高频部分还是低频部分,按照上述规则将采样点倒置,重构出来的信号与原信号相比有较大失真.但总的来说,在阈值相等的情况下,倒置高频部分系数后的重构信号比倒置低频部分的要好很多;而当阈值衰变到一定范围后又发现,在低频部分,将幅值高于 β 的采样点倒置后的重构信号效果相比于将幅值低于 α 的采样点倒置要差.而在高频部分恰恰相反,将幅值高于 β 的采样点倒置后的信号效果要比将幅值低于 α 的采样点倒置好.

相邻采样点幅值差:假设第 i 个采样点的幅值为 $p(i)$,设定一个幅差阈值 ε.我们做出如下规定:若该点的幅值与其左右相邻采样点幅值(也可采用左右各 l 个点幅值的均值)之差在阈值 ε 内(即 $|p(i)-p(i-1)|<\varepsilon$ 且 $|p(i+1)-p(i)|<\varepsilon$),则称该点为平稳点.否则称之为跳变点.经过实验我们发现,无论是在高频还是低频部分,在同样阈值 ε 下,将跳变点倒置后重构信号音质效果要比平稳点好,此外,阈值 ε 的选取也会影响重构信号的音质,当 ε 的取值低于采样点振幅均值时,重构信号的音质比较差,这种趋势在信号的低频部分中表现的尤为突出,在高频部分,这种变化相对平缓.

2.2.2 基于采样倒置和提升小波的秘密信息隐藏

设秘密信息为 S(S 表示原秘密信息经过预处理后形成的二进制序列),长度为 l_S,每一位秘密信息用 n 位小波系数来表示.选取一段长度为 l_V 载体信息为 V,(其中 $l_V \geqslant l_S * n * 2$).先将 V 进行一级提升小波分解,得到一组长度同为 $l_V/2$ 低频分量 cA 和高频分量 cD.选定一组 Logistic 初值作为隐藏密钥,利用这一组初值依次生成 $l_S * n$ 个取值范围在 $[1, l_V/2]$ 中的随机整数,将秘密信息隐藏到这些整数位置上的小波系数中去.为了获取最大的信息嵌入量,令 $n=1$.根据 S 中要嵌入的秘密信息通过倒置采样点的方法调整 cA、cD 中相应系数的极性,使得隐藏秘密数据为 1 时二者极性相同,为 0 时二者极性相反.

秘密信息的隐藏算法如下:首先找出各分量中恰好可以保证载体 V 听觉质量的一组阈值 α、β 和 ε.将 V 进行一级提升小波分解,利用随机序列选取其中需要修改的 l_S 个系数,分别将这些系数记为 $cA=\{A(i)\mid i=1,2,3\cdots l_S\}$ 和 $cD=\{D(i)\mid i=1,2,3\cdots l_S\}$.提取秘密序列 S 中当前需要嵌入的信息 $s(i)$,计算相应的 $A(i) * D(i)$,并按照以下规则对相应系数进行处理:

(1)隐藏秘密信息 1

■当 $A(i) * D(i) > 0$ 时,即 $A(i)$ 和 $D(i)$ 具有相同的极性.这种情况理论上不应该对其进行修改,但实际上信号在信道的传输过程中往往会伴随有自然的衰减或者遭遇有意无意的信号处理,会以一定的概率造成某些采样点幅值的变化,其结果容易导致秘密信息的误提取.由于本文采取的是一对一的单值信号隐藏方式,和均值隐藏方式不同,单值隐藏方式容易受到单个采样点幅值剧变的影响,为了将这种影响的风险降到最低,采用适度增加系数的方法来提高其鲁棒性,其具体方法如下:

假设 $A(i)>0$ 和 $D(i)>0$ 的情况,对于低频系数 $A(i)$ 来说,由于其保留了原信号的大部分能量,不可能对其进行较大幅度的修改,这里可以将载体信息低频部分的低倒阈值 α_A 近似看作是影响音频载体音质的临界阈值,预估计一个噪声门限 σ_A,一般来说 $\sigma_A < \alpha_A$,

这是因为如果 σ_A 的大小超过 α_A,意味着噪声已经影响了载体的可感知度.如果 $A(i)>\sigma_A$,就认为该系数是可靠的,不对其进行修改;如果 $A(i)\leqslant\sigma_A$,那么就说明 $A(i)$是不可靠的,其极性有可能因为干扰的原因而产生变化,所以这里通过给 $A(i)$增加一个较小的正值 Δ(本文中选取 $\Delta=(\alpha_A+\sigma_A)/2-A(i)$)的方式使修改后的 $A'(i)(A'(i)=A(i)+\Delta)$满足 $\sigma_A<A'(i)<\alpha_A$;对于高频系数 $D(i)$,也采用和低频系数同样的处理方法.类似的,在 $A(i)<0$ 和 $D(i)<0$ 的情况下,也采用和上述相同的处理方法.

■当 $A(i)*D(i)<0$ 时,即 $A(i)$和 $D(i)$具有相反的极性,这种情况下我们对这两个系数进行处理的方法是将其中一个系数倒置,使二者达到相同极性.考虑到对高频部分的倒置相对于低频部分来讲更容易保证载体信息的音质不受影响,所以理论上应该首选对高频部分系数进行倒置,但这种简单的处理得到的隐藏效果往往不尽如人意,因此在本文的算法中,笔者充分考虑了各种具体情况,给出了相应的处理策略.如表 1.

表 1　小波系数处理策略

$A(i)$ / $D(i)$	$\lvert A(i)\rvert\leqslant\alpha_A$		$\alpha_A<A(i)<\beta_A$		$\lvert A(i)\rvert\leqslant\beta_A$	
	跳变点	平稳点	跳变点	平稳点	跳变点	平稳点
$\lvert D(i)\rvert\leqslant\alpha_D$	倒置 $A(i)$	倒置 $D(i)$	倒置 $A(i)$	倒置 $D(i)$	倒置 $D(i)$	
$\alpha_D<\lvert D(i)\rvert<\beta_D$	倒置 $A(i)$		倒置 $A(i)$	倒置 $D(i)$	倒置 $D(i)$	
$\lvert D(i)\rvert\geqslant\beta_D$	倒置 $D(i)$		倒置 $D(i)$		倒置 $D(i)$	

■当 $A(i)*D(i)=0$ 时,若 $A(i)$、$D(i)$不同时为 0,采用前文中适度增加系数的方法对为 0 的一方进行处理,使之和不为 0 的一方处于相同极性.若 $A(i)$、$D(i)$同时为 0,那么就根据 cA 中正负系数的个数来调整 $A(i)$、$D(i)$的变化方式,若正系数的个数小于负系数,那么就用适度增加系数的方法使 $A(i)$、$D(i)$都变为正数,反之都变为负数,总而言之就是将 $A(i)$和 $D(i)$向正负系数中个数较少的一方变换.

(2)隐藏秘密信息 0

当隐藏秘密信息 0 时,对系数 $A(i)$和 $D(i)$的修改方法同隐藏信息 1 时大体相同,只不过是当 $A(i)*D(i)<0$ 时,修改方法对应隐藏 1 时 $A(i)*D(i)>0$ 的情况,当 $A(i)*D(i)>0$ 时,修改方法对应隐藏 1 时 $A(i)*D(i)<0$ 的情况,当 $A(i)*D(i)=0$ 时,和隐藏信息 1 时的不同只是变换结果应使两者处于不同极性.

对秘密序列 S 中的每一位都采取和上文相同的隐藏方法,将 l_S 个秘密信息分别隐藏到 V 中相应的 l_S 个位中去,在完成全部秘密信息的隐藏后,将修改过的系数代替原系数构造出新的低频分量 cA'和高频分量 cD',并利用 cA'、cD'重构出信号 V',并将 V'作为载密信息通过公共信道进行传输.

2.3　秘密信息的提取

相比于秘密信息的隐藏而言,其提取要相对简单一些.通过公共信道接收到 V'后,首先要对其进行预处理,即将 V'进行一级提升小波分解,得到其低、高频分量,然后通过提取密钥(一般情况下提取密钥和隐藏密钥相同)计算出混沌序列,找出秘密信息的嵌入位置 $cA'=\{A'(i)\mid i=1,2,3\cdots l_S\}$和 $cD'=\{D'(i)\mid i=1,2,3\cdots l_S\}$,计算相应位置的 $A'(i)*D'(i)$,并按以下规则提取出隐藏在其中的秘密信息:

$$A'(i)*D'(i)=\begin{cases}>0\ ,\ \text{提取秘密信息 1}\\<0\ ,\ \text{提取秘密信息 0}\end{cases}$$

将提取出来的二进制秘密序列解密,这样就完成秘密信息的提取过程.解密是加密的逆过程,设接收方接收到的秘密信息为 S'',长度为 $l_{s''}$.根据 $l^2\leqslant l_S<(l+1)^2$ 的原则计算出分组长度和组数 l,先将其中未被置乱的 S''_r 部分提取出来,然后根据密钥(即先前选定的那组 Logistic 混沌映射的初始值)计算出伪随机排列 C',将剩下的 S''_e 部分分为 l 个组后按照 C'的顺序进行反置乱得到 S_e,然后根据 S_e 和 S''_r 还原出原始秘密信息 S.

3　实验结果

3.1　实验环境和相关参数设定

(1)实验环境

硬件环境: Intel Pentium4 CPU 2.80GHz,1.00GB of RAM.**软件环境:**Microsoft Windows XP Professional Service Pack 3.**工作平台:**MATLAB v7.1.0.246 (R14) Service Pack 3.**秘密信息:**采样频率为 22kHz,量化位数为 8bit,PCM 编码的单声道 wav 格式音频信号,内容为女声普通话发音"晚上",时长 1s.**载体信息:**采样频率为 44kHz,量化位数为 16bit,PCM 编码的单声道 wav 格式音频信号,内容为一段音乐,时长 35s.

(2)实验参数:

根据实验测得载体信息的各项参数值如下:

$\alpha_A=0.09$、$\beta_A=1.43$、$\alpha_D=0.04$、$\beta_D=0.06$、

$\varepsilon=0.74$、$\sigma_A=\sigma_D=0.02$

在信息隐藏领域中,评价一个算法优劣的标准通常包括以下两个方面:不可感知性评价和鲁棒性评价.

3.2　不可感知性分析与评价

从客观和主观两个方面对载密信息的不可感知度进行分析和评价.首先比较载体信息和载密信息的时域特征,两者以及其差值的时域波形图如图 3.

由图 3 可以看到,原载体信号与载密信号整体波形差距不大,由于载密信号相对于原载体信号而言大量采用了采样点倒置的方式,因此其波形在局部没有原信号那么平滑.观察其差值可以发现,二者采样的主要差别

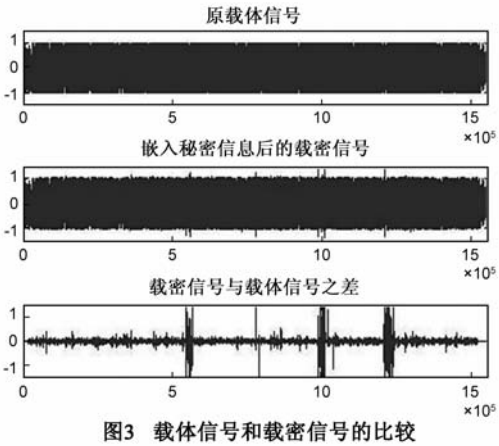


图3 载体信号和载密信号的比较

值点都集中在0轴附近,这是因为在处理过程中为克服噪声影响采用了适度增加系数的方法,表面上看这样做似乎是在原载体上加入了大量的噪声,理论上对原信号的声学特征必然会造成干扰,但事实上通过比较二者的听觉效果,发现这种干扰几乎不存在,究其原因在于引入了低倒阈值 α 的概念,根据2.2.1的分析,将幅值低于 α 的采样点倒置后的重构信号和原信号的听觉差异不大,观察差值波形,发现这些看似噪声的采样差基本上都在 α 之下,因此对原信号造成的影响在听觉方面几乎可以忽略.此外,还看到图中几个差值比较大的地方大都集中在原信号幅值较大且跳变点较多的区域,通过前文的分析,这些区域对原信号音质影响不大,其差别可以通过改变参数 α 和 ε 的值进行调节.因此,该载密信号和原信号相比具有良好的听觉相似度.

为了验证以上分析,在主观方面采用主观平均判分法对载密信息和载体信息的音质进行比较.对100人进行测试,得到如图4结果.90%的测试者认为载密信息和载体信息在听觉方面没有区别.

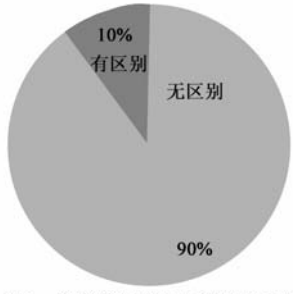


图4 载密信号的MOS测试结果

综上所述,可以得到以下结论:该算法在不可感知性方面具备良好的性能,隐藏信息给载体信息带来的影响是轻微的,人耳无法察觉.

3.3 鲁棒性分析与评价

鲁棒性也是评价算法优劣性的重要准则.本文针对加乘性噪声、采样频率变换、量化位数变换、压缩和解压缩等四种音频隐藏的攻击方式,对该算法进行鲁棒性分析和评价.

无攻击状态:不对载密信息进行任何处理,直接使用提取算法将其中的秘密信息提取出来,得到各项参数测试结果如表2.

表2 无攻击状态下各项参数的测试结果

SNR	BER	NC	MOS
30.936	0.000	1.000	5.0

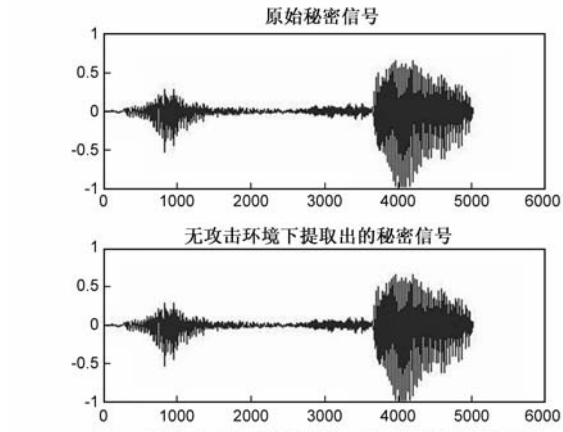


图5 无攻击状态下载体信号和载密信号的比较

根据表2和图5可以明显地发现,在无攻击的信道环境下,该算法可以0误码率提取秘密信息,提取出来的且秘密信息与原秘密信息在听觉方面没有差异.

噪声攻击:分别向载密信息中加入不同强度的均值噪声和高斯噪声.

表3 噪声攻击状态下各项参数的测试结果

噪声种类	噪声强度(方案)	SNR	BER	NC	MOS
均值噪声	0.001	30.885	0.000	1.000	5.0
	0.005	30.824	0.001	0.999	5.0
	0.01	30.791	0.001	0.999	5.0
高斯噪声	0.001	30.224	0.001	0.999	5.0
	0.005	30.003	0.002	0.999	5.0
	0.01	29.579	0.005	0.998	5.0

从表3和图6可以看出,由于该算法在秘密信息的隐藏过程中采用了预估噪声的策略,对均值噪声攻击具有非常好的鲁棒性.对于均值小于0.01高斯噪声来说,该算法也可以较好地从载密信息中提取秘密信息,当高斯噪声均值大于0.01时,其本身已经给载体信息带来较大的影响,在这种环境下,该算法依然能够很好地提取出具有完整语意的秘密信息.

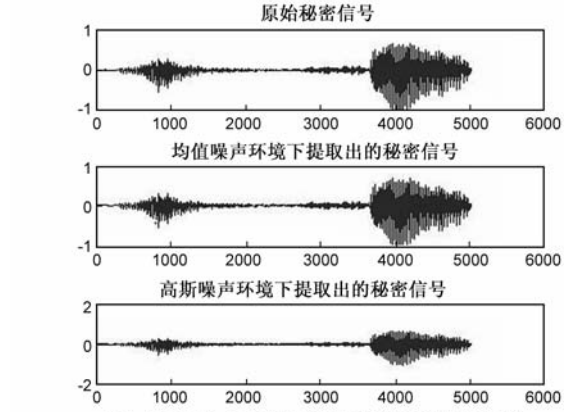


图6 噪声攻击下载体信号和载密信号的比较

重采样攻击:分别对载密信息进行上采样和下采样,前者先将载密信息的采样频率提高一倍以后再降低至原来的值,后者则是将载密信息的采样频率降低一倍以后再升高至原来的值.

从表 4 和图 7 发现,该算法在抵抗上采样和下采样方面存在较大的性能差异,其原因主要是因为上采样和下采样相比,采样点较原信号变化较大.而本文的算法核心恰恰是基于采样点的,因此上采样对本算法的冲击比较大,提取出来的秘密信息失真明显但基本可辨.

表 4　重采样攻击各项参数的测试结果

重采样类型	频率变化	SNR	BER	NC	MOS
上采样	44kHz ~ 88kHz ~ 44kHz	28.064	0.054	0.981	4.8
下采样	44kHz ~ 22kHz ~ 44kHz	29.301	0.001	0.997	5.0

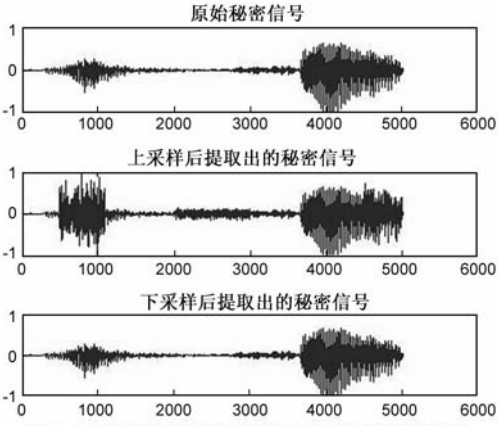


图7　重采样攻击下载体信号和载密信号的比较

重量化攻击:分别对载密信息进行升位量化和降位量化,前者先将载密信息的量化位数提高一倍以后再降低至原来的值,后者则是将载密信息的量化位数降低一倍以后再升高至原来的值.

表 5　重量化攻击各项参数的测试结果

重量化类型	量化位数变化	SNR	BER	NC	MOS
升位量化	16bit ~ 32bit ~ 16bit	29.419	0.002	0.998	5.0
降位量化	16bit ~ 8bit ~ 16bit	29.936	0.002	0.998	5.0

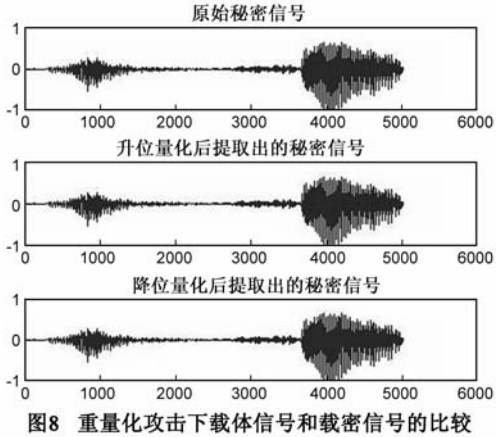


图8　重量化攻击下载体信号和载密信号的比较

从表 5 和图 8 可以看出,因为信号经过重量化后样本幅值的相对关系变化不大,本算法恰恰是利用了这一点,因此对重量化攻击也具有非常好的鲁棒性.

MP3 压缩攻击:将载密信息经 MP3 压缩后再解压.

从表 6 和图 9 可以看出,该算法在对 MP3 压缩同样具有较好的鲁棒性,提取出来的秘密信息清晰可辨,但由于 MP3 压缩本身的原因,载密信息的音质较原载体信息稍有差异.

表 6　MP3 压缩攻击各项参数的测试结果

SNR	BER	NC	MOS
29.222	0.001	0.999	4.2

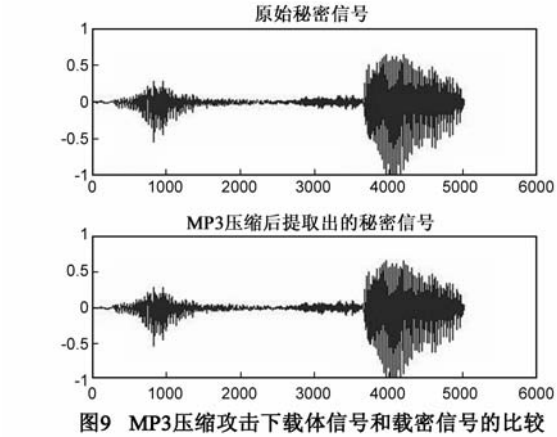


图9　MP3压缩攻击下载体信号和载密信号的比较

低通滤波攻击:使用 MATLAB 的 Cheby2 函数设计出契比雪夫Ⅱ型滤波器对载密信息进行滤波处理.

从表 7 和图 10 可以看出,因为该算法是采用判断小波高、低频分量相应位极性的方法来隐藏秘密信息的,由于低通滤波对信号的高频部分影响非常大,因此我们看到算法在这种攻击下的误码率相当高,即该算法对低通滤波攻击的鲁棒性不是很好.

表 7　低通滤波攻击攻击各项参数的测试结果

SNR	BER	NC	MOS
4.591	0.500	0.824	1.8

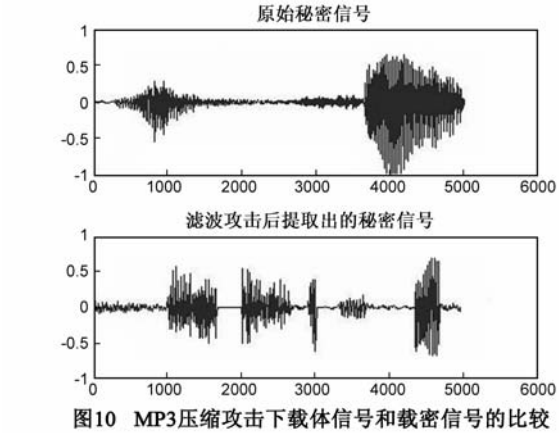


图10　MP3压缩攻击下载体信号和载密信号的比较

3.4 隐藏容量分析与评价

先前的大多数频域算法都是利用分组的方式,将秘密信息的每一位分别隐藏到各个组中去,根据每一组数据的统计特性来选择隐藏秘密信息的 1 或者 0.分组方式根据各自算法的不同也多有差异,从十几位到上百位不等,但总体来说都是以多个采样数据来表示秘密信息的一位.因此其容量一般只占原信号容量的很小一部分.本文提出了一种一对一的单值信号隐藏方式,大大增加了秘密信息的隐藏容量.

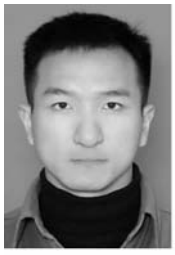
设有一采样频率为 44.1kHz 的载体信息,即其每秒的采样点数为 44100 个,就本文算法而言,因为秘密信息是隐藏在载体信息小波分解后的两个分量上,因此从理论上来说,本算法可以达到最大的隐藏容量为 44100/2 = 22050bps,这一点在同类算法中最好的,但在实际应用中,出于安全性或是不可感知性的需要,一般只选取部分系数进行隐藏,因此其隐藏容量一般是根据需要而变化的,即便如此,该算法在隐藏容量方面的优势仍然非常明显.

4 结语

本文通过使用了一对一的单值隐藏,大大增加了系统的隐藏容量.其间采用了设置低倒阈值和高倒阈值的方法,通过调整阈值的大小有效地控制了载密信息由于单值隐藏带来的感知上的失真.理论研究和实验结果表明,该算法不仅具有良好的不可感知性和鲁棒性,能够抵御除低通滤波攻击以外的其它攻击和信号处理,包括噪声攻击、重采样攻击、重量化攻击以及 MP3 压缩攻击等,而且信息隐藏容量大,可实现盲检测.因此,具有较高的实用价值.

作者简介:

谭 良 男,1972 年生,四川泸县人,博士,教授,研究方向为信息安全、云计算.
E-mail:tanliang@software.ict.ac.cn



吴 波 男,1983 年生,四川达州人,硕士,主要研究方向为信息隐藏.
E-mail:wubo_chn@yahoo.com

参考文献:

[1] R G van Schyndel, et al. A digital watermark[A]. Proceedings 1994 International Conference on Image Processing [C]. Austin, Texas, USA: IEEE Computer Society, 1994.2.86 – 89.

[2] Nedeljko Cvejic, Tapio Seppanen. Increasing the capacity of LSB-based audio steganography [A]. Proceedings of IEEE Workshop on Multimedia Signal Processing, 2002, St [C]. Thomas, Virgin Islands, 2002.336 – 338.

[3] XINL, YUHH. Transparent and robust audio data hiding in cepstrum domain[A]. IEEE International Conference on Multimedia and Expo (ICME)[C]. New York, USA, 2000.1.397 – 400.

[4] KIM H J, CHOI Y H. A novel echo-hiding scheme with backward and forward kernels[J]. Circuits and Systems for Video Technology, 2003, 13: 885 – 889.

[5] Nedeljko Cvejic, Tapio Seppanen. Spread spectrum audio watermarking using frequency hopping and attack characterization [A]. Signal Processing[C]. Elsevier North-Holland, 2004.84. 207 – 213.

[6] Kirovski D, Malvar H. Robust spread-spectrum audio watermarking[A]. Proceeding of IEEE ICASSP[C]. Salt Lake City, USA, 2001.3.1345 – 1348.

[7] Hartung F, Ramme F. Digital rights management and watermarking of multimedia content for m-commerce applications [J]. IEEE Communications Magazine, 2000, 38(11): 78 – 84.

[8] Paul Jessop. The business case for audio watermarking[A]. IEEE International Conference on Acoustics, Speech, and Signal Processing[C]. Phoenix, AZ, 1999.4.2077 – 2078.

[9] Solachidis V, Pitas I. Watermarking polygonal lines using Fourier descriptors[J]. IEEE Computer Graphics and Applications, 2004, 24: 1955 – 1958.

[10] 李赵红,侯建军.基于 Logistic 混沌映射的 DCT 域脆弱数字水印算法[J].电子学报,2006,34(12):2134 – 2137.
LI Zhao-hong, HOU Jian-ju. DCT-Domain fragile watermarking algorithm based on logistic map[J]. Acta Electronica Sinica, 2006, 34(12): 2134 – 2137. (in Chinese)

[11] 吴绍权,黄继武,黄达人.基于小波变换的自同步音频水印算法[J].计算机学报,2004,27(3):365 – 370.
WU Shao-Quan, HUANG Ji-Wu, HUANG Da-Ren. DWT-based audio watermarking with self-synchronization[J]. Chinese Journal of Computers, 2004, 27(3): 365 – 370. (in Chinese)

[12] Jim Chou, Kannan Ramchandran, Dan Sachs, Doug Jones. Audio data hiding with application to surround sound[A]. Proceedings of the 2003 IEEE Conference on Acoustics, Speech, and Signal Processing (ICASSP 2003)[C]. Hong Kong, 2003.337 – 340.

(下转第 1824 页)

[3] BLASER A D. Sketching Spatial Queries[D]. Maine: University of Maine, 2000.

[4] Ferri, Grifoni, Rafanelli. Querying by sketch geographical databases and ambiguities[A]. Copenhagen[M]. Denmark: Springer Verlag, 2005. 524 – 533.

[5] Ferri Grifoni, Rafanelli. The sketch recognition and query interpretation by GSQL, a geographical sketch query language[A]. Proceedings of the Fifth International Conference on Computer and Information Technology[C]. Washington, DC, USA: IEEE Computer Society, 2005. 34 – 38.

[6] 袁贞明,吴飞,庄越挺.基于草图内容的空间拓扑数据检索方法[J].浙江大学学报(工学版),2006,40(10):1663 – 1669.
Yuan Zhen-ming, Wu Fei, Zhuang Yue-ting. Spatial topological data retrieval based on sketch content[J]. Journal of Zhejiang University(Engineering Science), 2006, 40(10): 1663 – 1669. (in Chinese)

[7] Caduff D, Egenhofer. Geo-mobile query-by-sketch[J]. International Journal of Web Engineering and Technology, 2007, 3(2): 157 – 175.

[8] 王生生,刘大有,杨博.混合维定性空间查询语言[J].电子学报,2002,30(12A):1995 – 1999.
Wang Sheng-sheng, Liu Da-you, Yang Bo. Multi-imensional qualitative spatial query language MQS-SQL[J]. Acta Electronica Sinica, 2002, 30(12A): 1995 – 1999. (in Chinese)

[9] M J Egenhofer, R D Franzosa. Point-set topological spatial relations[J]. International Journal of Geographical Information Science, 1991, 2: 161 – 174.

[10] Goyal R, Egenhofer M J. The Direction Relation Matrix: A Representation for Directions Relations between Extended Spatial Objects[R]. Bar Harbor Maine: The Annual Assembly and the Summer Retreat of University Consortium for Geographic Information Systems Science, 1997.

[11] Goyal RK, Egenhofer MJ. Consistent queries over cardinal directions across different levels of detail[A]. 11th International Workshop on Database and Expert System Applications(DEXA'00)[C]. London, UK: IEEE Press, 2000. 876 – 880.

作者简介:

申世群 男,1977 年 4 月出生于黑龙江七台河,吉林大学计算机学院博士研究生,研究方向为时空推理,地理信息系统及其应用.
E-mail: shen_shiqun@163.com

刘大有 男,教授、博士生导师,1942 年 7 月生于吉林长春,现任吉林大学信息学部学部长和国务院学位委员会学科评议组成员等职务.主要研究知识工程和 ES,人工智能,时空推理,数据挖掘与统计关系学习,智能软件等.承担国家和省部级项目 40 余项,其中国家级 20 余项.发表论文 330 余篇,三大检索收录 200 余篇,出版著作 7 部.获国家科技进步二三等奖各 1 项,省部级科技进步一等奖 3 项、二三等奖 6 项.

王生生 男,1974 年生,博士,吉林大学教授,主要研究领域为时空推理、地理信息系统和语义 Web 等.

朱丽娜 女,1978 年生,硕士,沈阳炮兵学院讲师,研究方向为地理信息系统及其应用等.

(上接第 1818 页)

[13] Hafiz Malik, Ashfaq Khokhar, Rashid Ansari. Robust data—hiding in audio[A]. 2004 IEEE International Conference on Multimedia and Expro(ICME)[C]. Taipei, 2004. 959 – 962.

[14] 全笑梅,张鸿宾.基于小波包域听觉感知分析的统计音频水印算法[J].电子学报,2007,35 (4):673 – 678.
Quan Xiao-mei, Zhang Hong-bin. Statistical audio watermarking algorithm based on auditory analysis in wavelet packet domain[J]. Acta Electronica Sinica, 2007, 35(4): 673 – 678. (in Chinese)

[15] 孔涛,张丹.Arnold 反变换的一种新算法[J].软件学报,2004,15(10):1158 – 1164.
Kong Tao, Zhang Dan. A new anti-arnold transformation algorithm[J]. Journal of Software, 2004, 15(10): 1158 – 1164. (in Chinese)

[16] 林卫强,黄元石.Logistic 混沌序列的随机性分析[J].福州大学学报(自然科学版),2004,32(3):270 – 274.
Lin Wei-qiang, Huang Yuan-shi. Analysis for randomness of the series generated by chaos logistic system[J]. Journal of Fuzhou University, 2004, 32(3): 270 – 274. (in Chinese)