

# 基于音频载体的特定信息隐藏算法研究

姚 远, 白天皓, 李亚伟

(华中师范大学 物理科学与技术学院, 湖北 武汉 430000)

**摘 要:**无线通信技术的飞速发展推动移动终端间的数据业务日益增多,如何解决数据的传输安全显得尤其重要。为解决数据传输的安全问题,提出一种基于音频载体的特定信息隐藏算法。首先对特定信息进行随机密钥混沌加密和CRC编码处理来提高传输的安全性,之后对音频载体进行离散小波变换,取低频分量进行特定的分段处理,然后对每段数据进行SVD分解得到奇异值,对所有奇异值进行大小排序,将加密后的特定信息通过奇偶量化方法嵌入到较大的奇异值中。通信接收方收到音频数据后,通过对音频数据进行离散小波变换与SVD分解提取出嵌入的信息,之后进行CRC解码校验和混沌解密即可得到特定信息。实验结果验证了该隐藏算法在嵌入信息后具有不错的透明性,并且可以较好地抵抗常规攻击。

**关键词:**音频载体;信息隐藏;奇异值分解;离散小波变换;混沌映射

中图分类号:TP309

文献标识码:A

文章编号:1673-629X(2020)06-0104-05

doi:10.3969/j.issn.1673-629X.2020.06.020

## Research on Specific Information Hiding Algorithm Based on Audio Carrier

YAO Yuan, BAI Tian-hao, LI Ya-wei

(School of Physical Science and Technology, Central China Normal University, Wuhan 430000, China)

**Abstract:** The rapid development of wireless communication technology has promoted the increasing number of data services for mobile terminals, so how to solve the problem of data transmission security is particularly important. An information hiding algorithm based on audio carrier is proposed. Firstly, random key chaotic encryption and CRC encoding are performed for specific information to improve transmission security. Secondly, discrete wavelet transform is carried out on the audio carrier, and the low-frequency component is selected for specific segmentation processing. Then SVD decomposition is carried out on each data segment to obtain the singular value, and the size of all singular values is sorted. The encrypted specific information is embedded into the large singular value through the parity quantization method. After the communication receiver receives the audio data, the embedded information is extracted by discrete wavelet transform and SVD decomposition of the audio data, and then the specific information can be obtained by CRC decoding and chaos decryption. The experiment verifies that the proposed hidden algorithm has excellent transparency after embedding information and can resist normal attacks.

**Key words:** audio carrier; information hiding; singular value decomposition; discrete wavelet transform; chaotic mapping

## 0 引 言

随着网络技术的发展,移动终端的数据互传业务日益增多,攻击者可以利用网络传输的漏洞来窃取用户传输的私密信息,因此信息安全的问题显得尤其重要。近几年,信息隐藏技术<sup>[1]</sup>在信息安全领域迅速发展并取得了较多成果。语音作为人与人之间交流的重要载体,伴随着网络通信技术的进步,无线语音通信在人们生活中越发普遍,以音频为载体的信息隐藏技术

也日益成为研究热点。

音频信息隐藏可以分为音频水印<sup>[2-3]</sup>和音频隐写<sup>[4-5]</sup>两个分支。音频水印技术是版权保护领域的一种新技术,常见的音频水印算法主要包括时域<sup>[6]</sup>和变换域<sup>[7-8]</sup>两类。在时域进行信息隐藏具有嵌入信息量大,操作简便等优点,但是对攻击的抵抗性较差;变换域水印算法在保证不可感知性的前提下仍具有良好的鲁棒性,其中主要包括离散余弦变换、离散小波变换、

收稿日期:2019-07-18

修回日期:2019-11-20

基金项目:中央高校基本科研资助项目(CCNU18CG007, CCNU18TS030)

作者简介:姚 远(1974-),男,博士,副教授,硕士,主要从事信息处理、嵌入式系统应用、测控网络等相关领域的研究;白天皓(1995-),男,硕士研究生,研究方向为音频加解密。

傅里叶变换等。文献[9]结合小波变换与心理学模型,根据子带掩蔽阈值自适应地在小波域嵌入水印。文献[10]提出一种基于 DCT 域系数比较的音频盲水印算法,该算法具有良好的透明性,但是鲁棒性欠佳。文献[11]提出一种结合 DCT 变换与 SVD 分解的水印算法,在 DCT 域对音频进行 SVD 分解来实现水印嵌入,算法可以抵抗常见音频攻击。文献[12]分析了 DWT 变换与 SVD 分解的各自优势,通过对音频进行 DWT-SVD 变换,选择分解后的奇异值使用量化的方式嵌入水印。其算法的透明性与鲁棒性都具有不错的效果。文献[13]基于音频的 MFCC 特征,在音频小波域进行 SVD 分解嵌入脆弱水印,在抵抗多种攻击的同时可以定位恶意篡改位。

文中借鉴变换域的音频水印算法,结合离散小波变换(DWT)和奇异值分解(SVD)的特征,提出一种基于音频载体的特定信息隐藏算法。将整个音频载体进行离散小波变换,取近似分量部分按特定长度分段,每段系数进行 SVD 分解得到奇异值。因为矩阵奇异值越大其稳定性越好,该算法在得到奇异值后并没有直接进行嵌入,而是对所有奇异值进行排序,选择较大的奇异值以奇偶量化的方式嵌入信息。同时为了保证安全性,在嵌入前对特定信息进行混沌加密和 CRC 编码处理。实验结果证明该算法在不可感知和抵抗攻击方面都具有不错的效果。

## 1 基于音频载体的特定信息隐藏算法

### 1.1 特定信息预处理

为提高特定信息的安全性,在嵌入音频前对特定信息进行预处理操作,即进行混沌加密和 CRC 编码<sup>[14]</sup>。混沌是一个复杂的非线性非平衡动态过程,具有高度随机性和低通特性的同时能够有效抵抗有损压缩和低通滤波等攻击。Logistic 映射<sup>[15]</sup>是一种典型的混沌动力学系统,其方程为:

$$S_{n+1} = \mu * S_n * (1 - S_n) \quad (1)$$

其中,  $\mu$  为控制变量,  $S_n$  为混沌序列值且  $S_n \in (0, 1)$ ,  $S_0$  为序列  $S_n$  初始值。当  $3.57 < \mu < 4$  时,从初始值  $S_0$  开始迭代生成的 Logistic 混沌序列处于混沌状态。

为解决密钥固定导致安全性降低的问题,文中采用随机密钥加密方式对特定信息进行混沌加密。首先,加密方和解密方各约定好相同的索引库,索引库中存放了 256 对混沌 logistic 控制参数,即控制变量  $\mu$  和初始值  $S_0$ ,每一对参数都对应一个索引值(8 bit)。开始加密前先随机生成一个索引值,取出其在库中对应的参数来生成混沌序列,将生成的混沌序列与特定信息进行异或操作得到加密后信息。解密过程为:接受方提取出密文信息后,先取出前 8 bit 的密钥索引值,

进入索引库中搜索其对应的混沌 logistic 控制参数  $\mu$  和  $S_0$  生成混沌序列,与密文异或即可解密。

文中特定信息选择二值图像,先将二值图像降维成  $n$  位一维向量;之后在 256 个索引值中随机选择一个,在库中找到对应的控制参数  $\mu$  和  $S_0$ ,构建  $n$  位的 logistic 混沌序列,与一维的特定信息异或得到密文,将 8 bit 索引值放在  $n$  位密文前面得到  $n+8$  位最终密文。之后采用 CRC-16 编码生成 16 位校验码置于加密信息最后,经过处理的最终信息用元素  $w(i)$  表示,长度记为  $M$ 。

### 1.2 特定信息隐藏与提取

变换域信息隐藏算法由于其良好的鲁棒性被广泛应用。其中离散小波变换(DWT)可以从时间和频域角度同时对信号进行多尺度分析,相比于其他变换可以更有效地从信号中提取信息,故经离散小波变换后分解得到的信号低频分量更加精准,由于音频的能量大部分集中在低频区域,因此在其中隐藏信息可以大大提高鲁棒性。奇异值分解<sup>[16]</sup>(SVD)是一种将矩阵对角化的数值方法,具有很好的稳定性,表现在当矩阵的奇异值发生变动时,逆变换后的矩阵不会发生较大变化。在矩阵的奇异值中隐藏信息可以抵抗常见攻击,同时增加了隐藏信息后的透明性。经 1.1 节预处理得到加密的特定信息后,基于 DWT 和 SVD 将加密的特定信息隐藏到音频载体中,嵌入方法具体如下:

(1)对原始音频进行二级小波变换,取出小波变换后的低频分量  $Ca$ ,长度记为  $L$ 。对低频分量  $Ca$  以长度  $T$  进行分段,分段后每段构成一个  $1 * T$  的一维矩阵,记共分为  $a = L / T$  段。

(2)对每个  $1 * T$  矩阵进行奇异值分解,得到  $a$  个奇异值矩阵  $X$ ,选出每个奇异值矩阵  $X$  中的第一个元素  $X_1$ 。对所有分段的  $X_1$  进行对比排列,选择其中值最大的  $M$  个作为嵌入位置,进行特定信息嵌入。

(3)采取奇偶量化<sup>[17]</sup>的方式将特定信息  $w(i)$  嵌入到  $X_1$  中。每个  $X_1$  嵌入一比特特定信息,引入量化步长  $\Delta$  来提高鲁棒性。定义:

$$\text{temp} = \text{round}(X_1 / \Delta) \quad (2)$$

取  $\text{mod}(\text{temp}, 2)$  的值记为  $a$ ,嵌入特定信息如式(3)所示:

$$X_1 = \begin{cases} \Delta * \text{temp} & (w(i) = 1) \& (a = 1) \\ \Delta * (\text{temp} + 1) & (w(i) = 1) \& (a = 0) \\ \Delta * \text{temp} & (w(i) = 0) \& (a = 0) \\ \Delta * (\text{temp} + 1) & (w(i) = 0) \& (a = 1) \end{cases} \quad (3)$$

重复以上步骤将特定信息嵌入完毕后,对所有的奇异值矩阵  $X$  进行逆 SVD 变换得到分段的 DWT 系数向量。整合后对其二级逆小波变换,得到含特定信

息的音频数据。

特定信息提取流程如下所示:

(1)将原始音频数据进行二级小波变换,取出低频分量按长度  $T$  分段并进行 SVD 分解。对所有分段分解后的奇异值矩阵  $X$  中的元素  $X_i$  进行大小排序,选出最大的  $M$  个  $X_i$  所对应分段即为特定信息嵌入的位置。

(2)对含信息音频数据进行二级小波变换,取出低频分量按长度  $T$  分段,对上步筛选出来的分段进行 SVD 分解,取出  $X$  矩阵中元素  $X_i$  按以下公式进行

提取:

$$w(i) = \begin{cases} 1 & \text{mod}(\text{round}(X_i/\Delta), 2) = 1 \\ 0 & \text{mod}(\text{round}(X_i/\Delta), 2) = 0 \end{cases} \quad (4)$$

(3)将所有的嵌入分段按以上步骤提取后,先对提取的信息进行 CRC 解码判定提取的信息是否发生错误。若无误即可执行 1.1 节解密得到特定信息,反之则说明数据发生丢失或者修改,则通知发送方重新发送数据。文中算法隐藏与提取流程分别如图 1 所示。

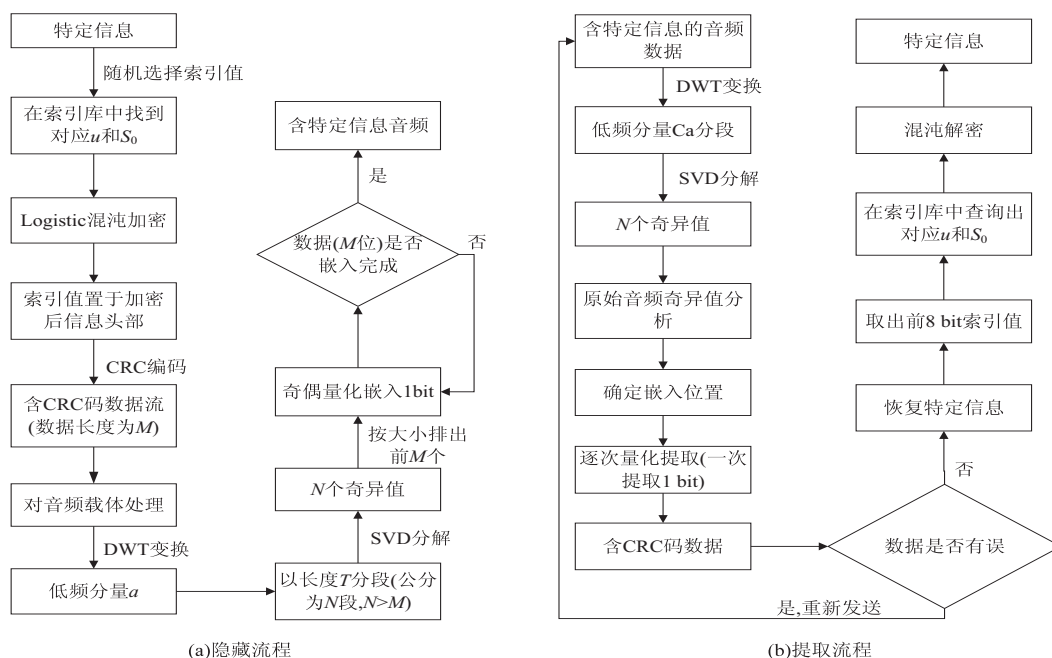


图 1 隐藏与提取算法

## 2 实验结果及分析

选择在 matlab2012a 环境下进行仿真,音频载体为采样频率 8 kHz、量化精度 16 bit 的单声道 WAV 音频信号,分段长度  $T=10$ ,量化步长  $\Delta=0.5$ 。测试的特定信息选择  $32 \times 32$  的二值图像 CCNU. bmp,原始图片和加密后图片见图 2。



图 2 原始和加密的特定信息

### 2.1 加密算法的性能分析

#### 2.1.1 密钥敏感性分析

加密算法要求必须对密钥有极高的敏感性。当密钥发生极其细微的变化时,密文都会随之发生巨大改变,这便是密钥的敏感性。分别对密钥  $\mu$  和  $S_0$  进行细微改变后,对相同明文数据进行加密,与原密钥加密后的密文进行对比,计算其密文变化比率,如表 1 所示。

#### 2.1.2 抗差分攻击分析

加密算法的攻击方式可以分为四种:唯密文攻击、已知明文攻击、选择明文攻击和差分攻击。差分攻击<sup>[18]</sup>是四种攻击方法中最有效的,如果加密算法可以抵抗差分攻击,那么其他的三种攻击也可以抵抗。差分攻击的做法是攻击者对明文数据进行微小改变后,利用加密算法改变前后的明文数据进行加密,通过对

表 1 密文变化比率程度表

$\mu$	$S_0$	密文变化
3.85 (原密钥)	0.6 (原密钥)	0.00%
3.850 000 001	0.6	98.04%
3.85	0.600 000 01	98.24%
3.850 000 001	0.600 000 01	98.04%

不同密文数据之间的差异可以分析出规律解出密钥。文中的加密算法由于为随机密钥方式,即改变明文后再加密时密钥已经改变,故可抵抗差分攻击。经过测试,选择 50 字节、100 字节和 200 字节明文数据,分别对仅改变 1 字节的两个明文进行加密,密文变化率分别为 97.95%、98.98%、98.93%,明文的稍许改变会带来密文的巨大变化,因此增加了差分攻击的难度。

2.2 特定信息隐藏算法性能分析

2.2.1 不可感知性检测

图 3 为原始音频和含特定信息的音频波形对比,对比波形图可以看出嵌入特定信息后音频数据基本无变动。分别采取主观测评与客观测评对不可感知性进行分析。

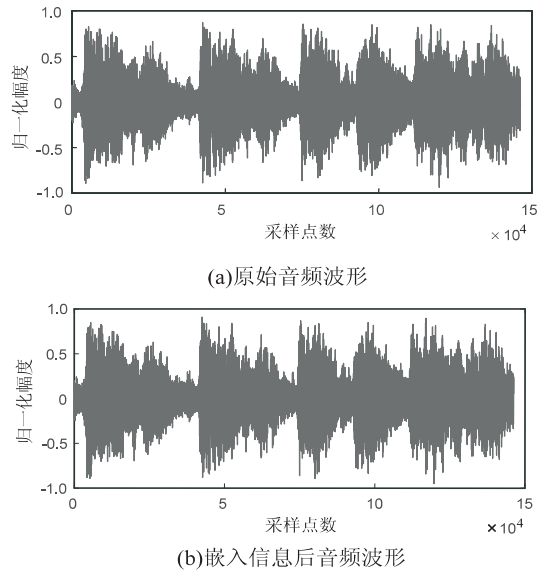


图 3 音频波形对比

主观测评采用最直观的方式对算法进行测试,直接听取嵌入特定信息后的音频载体,选择国际主流的 Subjective Difference Grades 标准 (SDG)。SDG 为 0 表示毫无差别,之后等级表示差别效果依次增大。选取 15 人的样本在安静的实验室环境下对以上两段音频进行评估,结果如表 2 所示。

表 2 主观测评

SDG	人数
0	14
-1	1
-2	0
-3	0
-4	0

客观测评标准为计算嵌入特定信息前后的信噪比,嵌入的特定信息可以看成添加噪声信号,当然这会对音频载体质量造成一定的影响。因此衡量嵌入的特定信息对原始音频造成影响程度的大小,就可以用信噪比的值的大小来表示。文中算法在测试音频类型分别选择流行音乐、古典音乐与摇滚音乐,嵌入特定信息后的信噪比分别为 16.699 9、16.336 9、16.107 8。

2.2.2 鲁棒性测试

为了测试算法的鲁棒性,对嵌入特定信息后的音频信号进行以下攻击测试:(1)加 20 dB 高斯噪声;(2)经过截至频率为 8 kHz 的低通滤波;(3)重采样:将采样率提升到 44.1 kHz 之后再降到 8 kHz;(4)MP3 压缩:以 128 kbit/s 的比特率进行 MP3 压缩,攻击之后提取水印信息。计算其相关系数 (NC) 和误码率 (BER) 并与文献[11]、文献[12]进行比较,表 3 为数据对比。

表 3 不同算法对音频攻击的鲁棒性

指标	无攻击	高斯噪声	低通滤波	重采样	MP3 压缩
文献[11]NC	1.000 0	0.930 8	0.984 7	0.984 7	0.987 8
文献[11]BER	0.00%	9.88%	2.19%	2.19%	1.75%
文献[11]算法提取					
文献[12]NC	1.000 0	0.956 2	1.000 0	1.000 0	0.984 7
文献[12]BER	0.00%	5.50%	0.00%	0.00%	1.81%
文献[12]算法提取					
文中 NC	1.000 0	0.996 3	1.000 0	1.000 0	0.995 3
文中 BER	0.00%	0.44%	0.00%	0.00%	0.56%
文中算法提取					



从表 3 中可以看出,文中算法相比文献[11]和文献[12]的算法在抵抗加高斯噪声和 MP3 压缩等攻击上都有明显提升,说明算法总体鲁棒性更强,有效降低了特定信息的误码率。

### 3 结束语

提出了基于音频载体的特定信息隐藏算法,将特定信息先进行混沌加密和 CRC 编码,再对加密后的特定信息隐藏在音频载体中实现保密通信。信息隐藏算法结合离散小波变换(DWT)和奇异值分解(SVD),在具有良好透明性的同时提高了鲁棒性。实验验证了该算法的有效性,为信息安全传输提供了一种较好的思路。

#### 参考文献:

- [1] SHI Y, LI X, ZHANG X, et al. Reversible data hiding: advances in the past two decades[J]. IEEE Access, 2016, 4: 3210–3237.
- [2] CAI C X, HUANG X H. An audio watermarking algorithm anti synchronization attack in DCT domain[J]. Journal of Optoelectronics · Laser, 2016, 27(3): 310–316.
- [3] HUA G, HUANG J, SHI Y Q, et al. Twenty years of digital audio watermarking – a comprehensive review[J]. Signal Processing, 2016, 128: 222–242.
- [4] LUO W, ZHANG Y, LI H. Adaptive audio steganography based on advanced audio coding and syndrome coding[C]// International workshop on digital watermarking. [s. l.]: [s. n.], 2017: 177–186.
- [5] 张 垚, 潘 峰, 申军伟, 等. 基于 MP3 的后置式自适应隐写算法[J]. 计算机科学, 2016, 43(8): 114–117.
- [6] 张一帆, 蒋天发. 基于时域扩展回声隐藏的数字音频水印研究[J]. 计算机工程与应用, 2008, 44(31): 119–120.
- [7] HU H T, HSU L Y, CHOU H H. Variable-dimensional vector modulation for perceptual-based DWT blind audio watermarking with adjustable payload capacity[J]. Digital Signal Processing, 2014, 31: 115–123.
- [8] HU H T, HSU L Y. Robust, transparent and high-capacity audio watermarking in DCT domain[J]. Signal Processing, 2015, 109: 226–235.
- [9] 张 涛, 张彩霞, 高新意, 等. 自适应的混合域音频水印新算法[J]. 信号处理, 2017, 33(6): 828–835.
- [10] 彭 维, 高 健, 孙瑞鹏, 等. 基于 DCT 系数比较的音频水印算法[J]. 计算机应用与软件, 2014, 31(11): 158–160.
- [11] 朱宪花, 雷 敏, 杨 榆, 等. 一种基于 DCT 和 SVD 的音频水印算法[J]. 计算机工程, 2012, 38(19): 111–113.
- [12] 段岁军, 范九伦. 一种基于 SVD 和 DWT 的音频水印算法[J]. 计算机应用研究, 2014, 31(7): 2116–2118.
- [13] 宋 慧, 李 晨, 田丽华, 等. 基于音频特征 MFCC 的混合域脆弱水印算法[J]. 计算机工程与设计, 2017, 38(7): 1885–1890.
- [14] 李辉景, 王淑琴, 任勇峰, 等. 基于 CRC 校验的高速长线 LVDS 传输设计[J]. 电子器件, 2015, 38(6): 1346–1351.
- [15] 吕 群, 薛 伟. 结合混沌系统和动态 S-盒的图像加密算法[J]. 小型微型计算机系统, 2018, 39(3): 607–613.
- [16] 冯小明, 冯乃光, 汪云云. 离散小波变换与奇异值分解的音频信号水印算法[J]. 华侨大学学报: 自然科学版, 2016, 37(6): 770–773.
- [17] 何选森, 陈 利, 吴良敏. 基于奇偶量化的图像水印嵌入与检测方法[J]. 电子测量与仪器学报, 2011, 25(12): 1041–1046.
- [18] 王 勇, 方小强, 王 瑛. 超混沌系统和 AES 结合的图像加密算法[J]. 计算机工程与应用, 2019, 55(8): 164–170.
- [19] (上接第 48 页)
- [20] 发现方法[J]. 计算机科学, 2018, 45(1): 216–222.
- [7] SOHN I, LEE J H, LEE S H. Low-energy adaptive clustering hierarchy using affinity propagation for wireless sensor networks[J]. IEEE Communications Letters, 2016, 20(3): 558–561.
- [8] 赵 昱, 陈 琴, 苏一丹, 等. 基于邻域相似度的近邻传播聚类算法[J]. 计算机工程与设计, 2018, 39(7): 1883–1888.
- [9] GUO W F, ZHANG S W. A general method of community detection by identifying community centers with affinity propagation[J]. Physica A: Statistical Mechanics & Its Applications, 2016, 447: 508–519.
- [10] SHANG R H, LUO S, ZHANG W T, et al. A multi-objective evolutionary algorithm to find community structures based on affinity propagation[J]. Physica A: Statistical Mechanics and Its Applications, 2016, 453: 203–227.
- [11] 王 林, 董小江. 社团挖掘的并行化 AP 聚类方法[J]. 微型机与应用, 2017, 36(12): 16–18.
- [12] 周春霞, 周井泉, 常瑞云. 基于 Memetic 算法的多目标复杂网络社区检测[J]. 计算机技术与发展, 2016, 26(1): 53–57.
- [13] 佟 鑫. 基于近邻传播的多目标进化算法及其应用[D]. 哈尔滨: 哈尔滨工业大学, 2015.
- [14] WANG F F, ZHANG B H, CHAI S C. Deep auto-encoded clustering algorithm for community detection in complex networks[J]. Chinese Journal of Electronics, 2019, 28(3): 489–496.
- [15] MENG Y Y, LIU X Y. Quantum inspired evolutionary algorithm for community detection in complex networks[J]. Physics Letters A, 2018, 382(34): 2305–2312.
- [16] MONDAL S A. An improved approximation algorithm for hierarchical clustering[J]. Pattern Recognition Letters, 2018, 104: 23–28.