基于混沌和小波变换的音频加密算法

魏雅娟 范九伦 任 方
(西安邮电大学通信与信息工程学院 西安 710061)

摘 要 为使音频信息可以在信道中安全传输,提出了一种在MPEG压缩的背景下基于混沌和小波变换的音频加密算法。首先对信号采用随机矩阵进行扩充来改变原信号的幅值,其次在"时域-小波域-时域"利用Logistic混沌映射进行3次音频信号置乱和扩散加密操作,最终得到加密信号。通过分段Logistic映射生成密钥的随机矩阵。理论分析发现,所提算法的密钥空间明显增大。实验结果表明,得到的音频加密信号的直方图分布更均匀,信号间的相关度变小,密钥敏感度增强。因此,提出的音频加密算法具有较高的安全性。

关键词 音频信号加密,混沌映射,小波变换,置乱,随机矩阵
中图法分类号 TN918.4 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2017.012.019

Audio Encryption Algorithm Based on Chaos and Wavelet Transform

WEI Ya-juan FAN Jiu-lun REN Fang
(School of Communication and Information Engineering, Xi'an University of Posts and Telecommunications, Xi'an 710061, China)

Abstract To make audio information broadcast across the Web safely, an audio encryption algorithm based on chaotic systems and the wavelet transform in MPEG background was proposed. Firstly, the signal is added with a random matrix to change the value of signal. Secondly, logistic map is used to scramble and diffuse the position of each signal in time and the wavelet domains for three times. Finally, we can obtain the secure signal. The random matrix used as keys was generated by piecewise Logistic map and the random seeds. The experiment results show the mentioned algorithm not only makes gray histogram uniform and signal correlation weake, but also increases key space and high sensitivity to the keys. Therefore, the audio encryption algorithm has higher security to protect audio information.

Keywords Audio information encryption, Chaotic map, Wavelet transform, Position scrambling, Random matrix

1 引言

快速更新的移动通讯设备和多媒体技术使得多媒体数据本身的安全问题受到广泛关注[1-2],例如,个体间的视音频通话或会议(包括视频数据和音频数据)不得被无授权的第三方获取和篡改;视频点播VOD系统中,只有付费的用户才可点播观看加密后的电视节目(视频数据和音频数据)等[3-4]。由此可见,音频数据在多媒体数据中的地位举足轻重,若无值得信赖的安全加密算法或系统保护,大量的原始音频信号将暴露于公开和共享的网络平台,从而对传递信息用户的隐私造成不可估量的影响[5]。因此,探讨高安全级别的音频信号加密算法成为一个重要的研究课题。

不同于文本、图像信息,相邻的音频信号间具有更大的冗余和更强的相关性。因此,音频加密与文本、图像加密算法不尽相同。最早的加密算法是由Phillips等[6]提出的基于振幅域的模拟音频加密算法,随后Jayant等[7]提出基于时域和频域的模拟音频加密算法,Liu等[8]提出针对数字音频的基于混沌系统块加密算法。

值得注意的是,音频信号中往往存在特殊的语音、语调或长时间的停顿,在信道传播过程中,有经验的攻击者往往会根据这些特殊性质进行推测判断,一旦识别成功就很容易对原始音频进行篡改,从而威胁音频数据的安全。

另外,无论是模拟音频数字化还是数字音频,其数据量相对庞大,不利于传输和存储,因此对数字音频进行压缩处理是必要的。本文在MPEG音频压缩的背景下提出一种基于混沌和小波变换的音频信号加密算法,该算法旨在解决信号中含有可供理解的特殊信息从而使音频信号易遭受攻击的问题。经本算法加密后的信号具有密钥空间大、密钥敏感度强、抗攻击且防篡改、解密后可得到高质量的解密信号等优势。

到稿日期:2016-10-09 返修日期:2016-12-25 本文受国家自然科学基金资助项目(61671377,61472472),陕西省自然科学基础研究计划资助项目(2015JQ6262),陕西省教育厅专项科研计划资助项目(15JK1669)资助。
魏雅娟(1991—),女,硕士生,主要研究方向为信息安全,E-mail:Virginia_wyj@163.com;**范九伦**(1964—),男,教授,博士生导师,主要研究方向为模式识别、信息安全;**任 方**(1981—),男,博士,副教授,主要研究方向为密码学、信息安全。

2　基础知识

2.1　数据压缩

2.1.1　PCM 编码技术

由数字技术的发展历史可知，PCM(Pulse Code Modulation)编码技术已被提出几十年。作为模拟信号与数字信号的接口，该技术的原理是将时间和幅度上连续变化的模拟信号转化为时间和幅度上离散的数字信号，以便在数字领域对信号进行处理、传输、存储等[9]。

PCM 包含取样、量化和编码 3 个步骤。该技术的优点是简单可行。采用 PCM 编码技术的音频信号为 WAV 音频信号，所提算法使用的实验音频均为 WAV 格式。WAV 文件由 RIFF WAVE 块、Format 块、Fact 块、Data 块组成，其中 Format 块含有音频的主要信息，其结构如表 1 所列。

表 1　Format 块结构

Name	Length/bytes	Content	Reference
ID	4	'fmt'	
Size	4	18/16 (有无附加信息)	本结构大小 (除 ID,Size)
Format Tag	2	通常 0x0001	编码方式
Channels	2	1-单声道； 2-双声道立体声	声道数目
SamplesPerSec	4	/	采样频率
AvgBytesPerSec	4	/	每秒所需字节数
Block Align	2	数据块对齐单位	
BitsPerSample	2	/	每个采样需要的 位 bit 数
附加信息	2	(可选，通过 Size 判断)	附加信息

然而，PCM 也存在如下不足：1)PCM 编码后生成的数据量非常大，对存储器的容量要求较高；2)传输信号所占用的信道带宽比模拟信号更大(直接传输模拟信号仅需 20kHz 带宽，而 PCM 编码的数字信号是其 35 倍以上)。因此，减少传输数字信号的数据量、降低带宽并保持信号原有质量的压缩编码方案应运而生。

2.1.2　MPEG-1 音频压缩

目前，众多学者比较认同的数据压缩分为某种程度上可逆与不可逆两类，分别被称为冗余度压缩与熵压缩，即无损压缩与有损压缩[10]。图 1 为数据压缩技术的简单分类示意图。

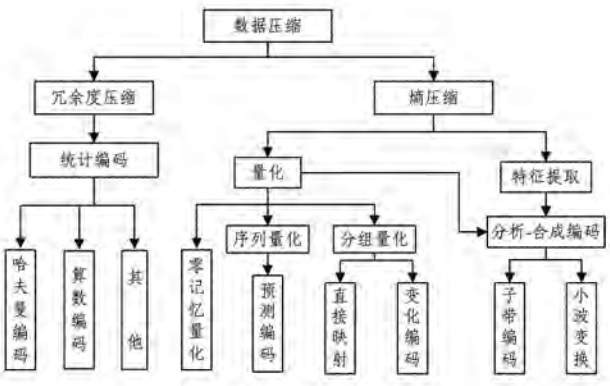


图 1　数据压缩技术简单分类

ISO/IEC 于 1990 年提出 MPEG-1 音频压缩标准，该标准属于有损压缩[11]。其音频编码分为 Layer1，Layer2，Layer3 3 个层次，层级越高，压缩效果越好，伴随编解码的复杂性也就越高 。

目前最为常用的压缩层级为 MPEG-1 Layer3(即 MP3)，被用于互联网的高质量音频传输。MP3 的编码流程如图 2 所示。该过程大致可分为：时频映射(包括子带滤波器组和 MDCT)和量化编码(包括比特、比特因子分配和哈夫曼编码)等。

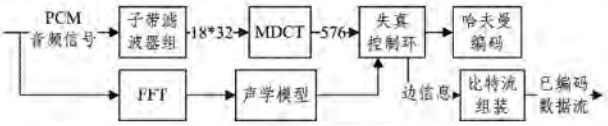


图 2　MP3 编码算法的流程图

本文提出的音频加密算法是在 MPEG-1 Layer3 的背景下对音频进行加密操作后再进行压缩，最后再在信道内传播到达信宿。

2.2　混沌映射与小波分解

2.2.1　混沌映射

Logistic 映射是非常著名的一维混沌映射，其形式简单且具有复杂的动力学行为，最早被广泛用于加密算法和伪随机位发生器的设计中。相对于传统加密算法，基于 Logistic 映射的加密算法的加密速度更快，效率更高，安全性更好[12]。其公式定义如下：

$$f(x_k)=x_{k+1}=\mu\cdot x_k\cdot(1-x_k) \tag{1}$$

其中，状态变量 $x_k\in(0,1)$，k 为迭代次数，参数控制 $\mu\in[0,4]$，混沌域为(0,1)。当 $3.5699456<\mu\leqslant 4$ 时，Logistic 映射处于混沌区域。

通过对传统 Logistic 映射的不足进行改进，结合分段 Tent 混沌映射，文献[13]提出了一种分段 Logistic 混沌映射。分段 Logistic 混沌映射的性能优于传统的 Logistic 映射，具有更为随机的分布和初值更为敏感等特性，其定义如下：

$$x_{n+1}=\begin{cases}4\cdot\mu\cdot x_n\cdot(0.5-x_n), & 0\leqslant x_n\leqslant 0.5\\ 1-4\cdot\mu\cdot x_n\cdot(x_n-0.5)\cdot(1-x_n), & 0.5<x_n\leqslant 1\end{cases} \tag{2}$$

与 Logistic 映射相似，定义状态变量 $x_k\in(0,1)$，k 为迭代次数，参数控制 $\mu\in[0,4]$，混沌域为(0,1)。

2.2.2　小波分解

小波分解可以通过 Morlet 算法实现，其算法表述为：

$$\begin{cases}c_{j+1}=Hc_j\\ d_{j+1}=Gc_j\end{cases},j=0,1,\cdots,J \tag{3}$$

其中，H 和 G 分别为一个低通滤波器和一个高通滤波器。将 c_0 定义为原始信号 X，通过式(3)可将 X 分解为 $d_1,d_2,\cdots,d_J$ 和 c_J(J 为最大分解层数)。图 3 为小波分解示意图，其表达式为[14-17]：

$$X=c_0=d_1+d_2+\cdots+d_J+c_J \tag{4}$$

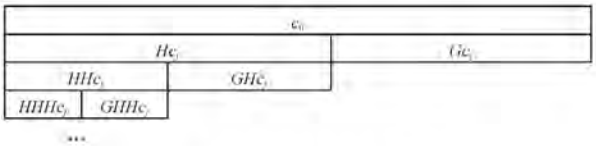


图 3 小波分解示意图

3 音频加密算法

本文提出的音频加密算法包括时域和小波域内的处理，在各自域内分别进行置乱和扩散操作。

预处理：由于音频信号长度不固定，为了便于计算，本算法首先在长度为 L_0 的音频后添加一个随机的一维扩充矩阵 l，新的一维音频信号长度为 $L_1=L_0+l$，其中 L_1 易转化为二维方阵 $F_2^{k\times k}$，以便后续的计算操作；然后再对新的一维音频信号加上一维随机掩膜矩阵，以修饰原音频中的特殊音素。

所提加密算法的流程如图 4 所示。

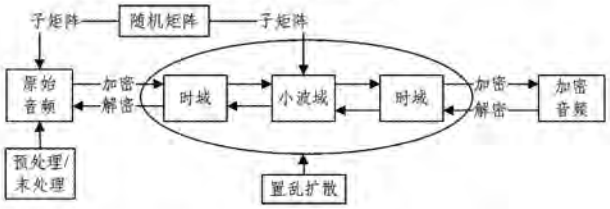


图 4 所提算法的加解密过程

3.1 算法中的随机矩阵

所提算法涉及的随机矩阵分别为一维扩充矩阵、一维掩膜矩阵和 4 个不同长度的一维掩膜子矩阵。上述矩阵均可通过一维掩膜矩阵简单变化得到。

一维掩膜矩阵通过分段 Logistic 映射生成，其长度为 $k*k$。使用分段 Logistic 映射的原因在于，其参与加密后得到的加密音频相关度低于使用传统的 Logistic 映射所生成的矩阵。

扩充矩阵是一维掩膜矩阵的子矩阵，其长度与原音频长度相加后恰好可以转化为二维方阵。

4 个不同长度的一维掩膜子矩阵是由一维掩膜矩阵左右翻转后(令矩阵长度 $L=k*k$)所得到的矩阵，以及取该矩阵的$[1,\frac{L}{2}]$,$[\frac{L}{2}+1,\frac{3}{4}L]$,$[\frac{3}{4}L+1,\frac{7}{8}L]$即可得到 4 个不同长度的一维掩膜子矩阵。

在音频信息中使用随机矩阵的原因：1)便于加密算法的处理操作；2)修饰音频中的特殊音素，避免有经验的攻击者通过统计分析来得到明文的相关信息。

3.2 置乱过程

所提算法中的置乱使用传统的 Logistic 混沌映射，共置乱 3 次：1)添加一维掩膜矩阵后，对加掩膜的矩阵在时域内进行置乱；2)在小波域内对 4 个分解矩阵分别进行置乱；3)在逆小波变换后，对得到的矩阵在时域内进行置乱。

使用传统的 Logistic 混沌映射进行置乱的原因在于，生成的混沌序列是为了将音频分为两部分，序列的随机性对加密效果的影响不大，因此使用传统的 Logistic 映射提高了算法的效率。

算法 1 置乱算法

1. 利用参数 μ，x_0 生成一维 Logistic 混沌序列，其中状态变量 $x_0\in(0,1)$，参数控制 $\mu\in[0,4]$。
2. 将混沌序列中 $x_k\geqslant 0.5$ 的数据的行(列)序号存入矩阵 series1，将 $x_k<0.5$ 的数据的行(列)序号存入矩阵 series2，这两个矩阵均为一维矩阵，存储的是混沌序列的序号。
3. 对于需要置乱的一维矩阵 sig，将 series1 和 series2 中的序号对应到 sig 中，提取序号对应的数据，并存入两个一维矩阵 M，N 内。
4. 将 M，N 合并，M，N 的前后顺序为：当置乱次数 m 为奇数时，M 置于 N 之前；当置乱次数 m 为偶数时，M 置于 N 之后。
5. 将合并的一维矩阵与对应的一维掩膜子矩阵求和，即可得到最终的置乱结果。

值得注意的是，已知原音频信息的幅值分布在[−1，1]之间，在加密过程中对它加上对应的掩膜矩阵后会出现幅值过大的情况，因此为了避免加密幅值过大导致后续处理的不便，我们将幅值超过 1 的部分减 2，小于 −1 的部分加 2，以将置乱后音频信息的幅值控制在[−1，1]之间。由于算法拥有记忆功能，因此解密时可以完全恢复音频信号。

置乱过程的流程图如图 5 所示。

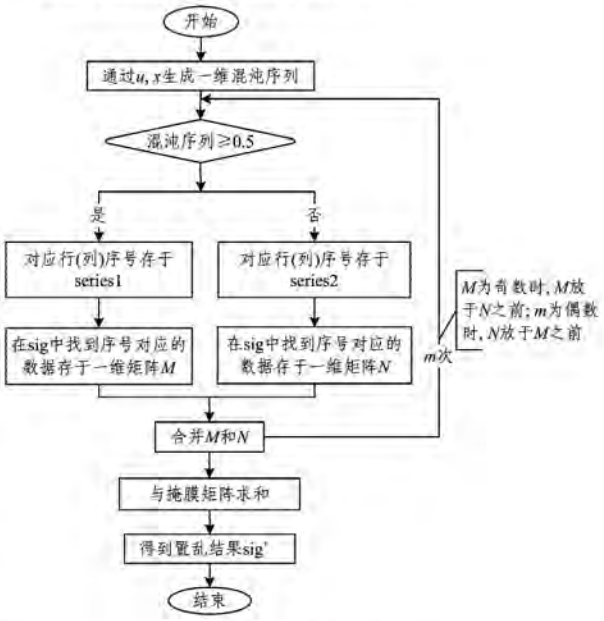


图 5 置乱过程

3.3 算法步骤

加密算法和解密算法分别如算法 2 和算法 3 所示。

算法 2 加密算法

1. 首先通过分段 Logistic 映射生成一维掩膜矩阵 A_1，通过 3.1 节所述的操作方法得到一维扩充矩阵 A_2 和 4 个长度不同的一维掩膜子矩阵(D_1，D_2，D_3，D_4)。在原始一维音频矩阵 y_1 末尾添加一个一维扩充矩阵 A_2，得到新的一维矩阵 B_1，然后加上与 B_1 等长的一维掩膜矩阵 A_1，进而得到一维矩阵 C_1。
2. 一次加密：在时域内对 C_1 进行置乱(其中一维掩膜子矩阵为 D_1)，进而得到一维矩阵 E_1。
3. 二次加密：首先对一维矩阵 E_1 进行一维小波变换，分解层数为 3，

得到 6 个一维分解矩阵 ca_1，cd_1；ca_2，cd_2；ca_3，cd_3（ca_1 可分解为 ca_2，cd_2；ca_2 可分解为 ca_3，cd_3），其中 ca 代表高频，cd 代表低频。分别对 cd_1；cd_2；ca_3，cd_3 在小波域内进行置乱（其中掩膜分别为 D_2，D_3，D_4），然后逆小波变换得到一维矩阵 E_1_en。

4. 三次加密：对 E_1_en 进行置乱（该过程无需加掩膜）后，最终得到一维加密音频矩阵 y_en。

算法 3　解密算法

1. 一次解密：将得到的一维加密音频矩阵 y_en 逆置乱，得到一维矩阵 y_dec。

2. 二次解密：首先对 y_dec 进行一维小波变换，分解层数为 3 层，得到 6 个一维分解矩阵 CA_1，CD_1；CA_2，CD_2；CA_3，CD_3。分别对 CD_1；CD_2；CA_3，CD_3 在小波域内进行逆置乱，然后逆小波变换得到一维矩阵 E_1_dec。

3. 三次解密：E_1_dec 在时域逆置乱后减去掩膜矩阵 A_1，并剔除加密时添加的扩充矩阵 A_2，从而得到最终解密的音频即原始音频 y_1。

4　算法分析

算法分析包括对算法的理论分析和对实验结果的分析。理论分析是对算法的密钥空间大小进行分析；实验结果分析包括 MOS 评估、统计分析（相关度系数、直方图）、密钥敏感度测试。分析结果表明，该算法的加密效果具有一定的鲁棒性，可使音频在信道内安全传输。

4.1　密钥空间

一个安全的加密系统应具有足够大的密钥空间来抵御穷举攻击[18]。

所提算法使用的密钥如下：算法中一维掩膜矩阵的行（列）数 k，生成掩膜矩阵所涉及分段混沌映射的参数 μ 和 x，置乱次数 m 和置乱使用的 Logistic 映射参数 μ_0，x_0，μ_1，x_1（前者用于时域，后者用于小波域），即：$\{k, \mu, x, m, \mu_0, x_0, \mu_1, x_1\}$。其中，$k$ 的取值范围为 $[100, 1000]$，$m \in [1, 100]$，$\mu \sim \mu_1$ 与 $x \sim x_1$ 的取值为小数，其取小数点后的 1 位至 30 位，则所提算法的密钥空间为以上子密钥的密钥空间的乘积。

在上述子密钥中，所有生成混沌序列的初始参数为主要密钥，即 $\mu \sim \mu_1$，$x \sim x_1$ 为算法主密钥。表 2 列出了主要密钥小数位的长度与算法的总密钥空间的对比。由表 2 可知，所提算法有足够大的密钥空间，可抵御穷举攻击。

表 2　所提算法主密钥小数点后的位数与总密钥空间的对比

主密钥小数点后的位数	密钥空间
3	1×10^{23}
6	1×10^{41}
9	1×10^{59}
20	1×10^{125}
30	1×10^{185}

4.2　MOS 评估

MOS 值作为衡量通信系统语音质量的重要指标，常被用来评价系统输出信号的话音质量。评价结果采用分数来衡量，分数取值为 0 到 5 之间的整数，0 表示最差的质量，5 表示质量无损。由于加密后的音频是杂乱无章的噪声，因此其 MOS 应趋于 0。

在计算 MOS 前应先计算倒谱距离。设 C_x 为原音频的倒谱系数，C_y 为加密后音频的倒谱系数，则倒谱距离[19-20]为：

$$CD=10\log_{10}[2*(C_x(i)-C_y(i))^2]^{\frac{1}{2}} \tag{5}$$

MOS 的评估公式为[19]：

$$MOS=0.0415CD^2-0.8010CD+3.5620 \tag{6}$$

其中，经过 MOS 评估的加密信号值不可超过 3.5，否则视其为音频加密效果不佳。

表 3 列出了不同音频分别经过所提算法和传统算法加密后的 MOS 评估结果。由表 3 可知，经过所提算法加密的音频的 MOS 值均小于 1，表明加密信号在信道传播过程中与加密前相比其语音质量极差，达到了较好的加密效果。

表 3　不同音频加密后 MOS 的评估结果

加密音频	Ding. wav	Ring01. wav	Ring06. wav	Ring10. wav
所提算法	0.9642	0.8452	0.7743	0.8107
传统算法	1.3682	0.9963	1.1523	1.2857

4.3　统计分析

攻击者为了获取明文信息，常对密文进行统计分析。在此，对该算法加密的音频进行统计分析，结果表明加密后的音频具有优良的置乱和扩散效果，足以抵御暴力统计分析。统计分析数据如下：

1）原音频信息和加密信息各自的相关度系数；

2）原音频信息和加密信息的直方图。

4.3.1　相关度系数

为了计算音频信息的相关系数，本文分别随机选取 1000 对相邻的音素进行统计分析。相关系数的计算公式如下[21]：

$$E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i \tag{7}$$

$$D(x)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))^2 \tag{8}$$

$$cov(x,y)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))(y_i-E(y)) \tag{9}$$

$$r_{xy}=\frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{10}$$

其中，x，y 分别是音频中相邻两音素的幅值。相关度系数越小，说明加密效果越好。

表 4 列出了原始音频的相关度、分别经传统算法和所提算法加密后信号的相关度，以及解密后音频间的相关度的对比结果。

表 4　邻域音频相关度分析

音频	原始音频	加密音频		解密音频	
		传统算法	本文算法	传统算法	本文算法
Ring01. wav	0.9833	0.0028	−0.0131	有噪声	0.9833
Ring06. wav	0.9930	−0.0083	0.0031	有噪声	0.9930
Ring08. wav	0.9842	0.0018	0.0057	有噪声	0.9842
Ring10. wav	0.9795	0.0199	−0.0065	有噪声	0.9795
Ding. wav	0.9722	0.0047	−0.0190	有噪声	0.9722

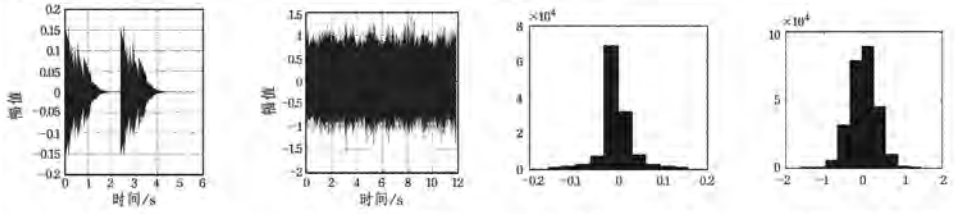
传统算法是指音频在 DCT 域或 DST 域内进行加密的算法（其中置乱过程与本算法相同）。

通过对比传统算法和所提算法分别加密后的音频信号的

相关度发现，经所提算法在小波域处理得到的结果优于其他频域处理得到的结果，加密后的音频相关度更低，这表明所提算法的加密效果优于传统加密算法。

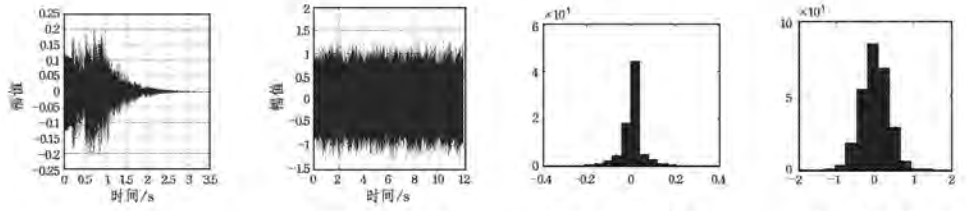
4.3.2 直方图

图 6—图 10 分别为原音频、加密后的音频的波形和直方图。



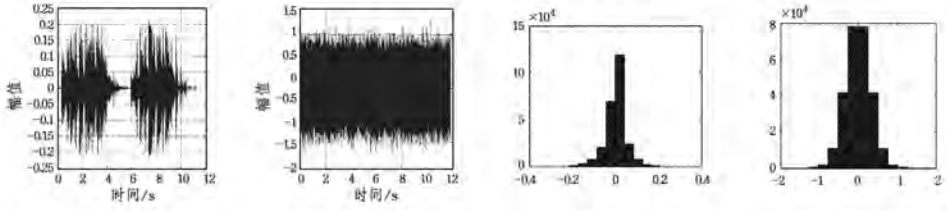
(a)原始音频 (b)加密后的音频 (c)原音频的直方图 (d)加密后的直方图

图 6 音频 Ring01.wav 的对比加密结果



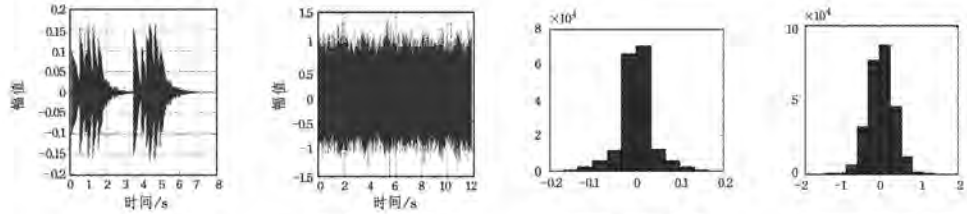
(a)原始音频 (b)加密后的音频 (c)原音频的直方图 (d)加密后的直方图

图 7 音频 Ring06.wav 的对比加密结果



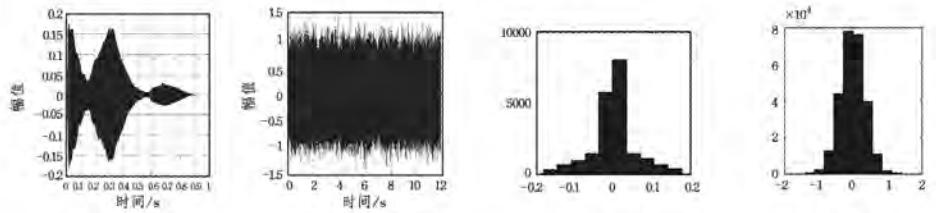
(a)原始音频 (b)加密后的音频 (c)原音频的直方图 (d)加密后的直方图

图 8 音频 Ring08.wav 的对比加密结果



(a)原始音频 (b)加密后的音频 (c)原音频的直方图 (d)加密后的直方图

图 9 音频 Ring10.wav 的对比加密结果



(a)原始音频 (b)加密后的音频 (c)原音频的直方图 (d)加密后的直方图

图 10 音频 Ding.wav 的对比加密结果

通过对比加密前后的波形图发现加密后的波形已无明显的原音频波形的痕迹。

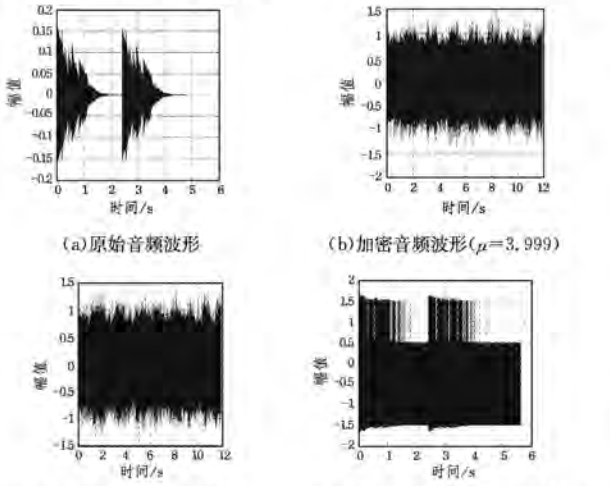
通过对比加密前和加密后的直方图可以看出，加密前的音频幅值分布在[−0.2,0.2]之间，加密后的时域直方图音频幅值分布在[−2,2]之间，且音素分布较均匀，因此算法可以有效地抵御统计攻击。

4.4 密钥敏感度分析

在密码学中，衡量加密算法的一项重要指标为雪崩效应[22]。严格雪崩效应指出，当改变明文或密钥中的任意 1 位时，几乎所有的密文数据都将发生变化。实验将产生掩膜矩阵的 $\mu(\mu=3.999)$增大 10^{-9}，变为 3.999000001，并用原始和增大后的密钥分别进行加密。另外，若使用原密钥加密，则使

用增大后的密钥解密时无法得到原始音频。

图 11 给出了密钥敏感性测试的音频波形图。该图表明算法密钥具有较强的密钥敏感性。



(a)原始音频波形　(b)加密音频波形(μ=3.999)

(c)加密音频波形(μ=3.999000001)　(d)错误密钥解密(μ=3.999000001)

图 11　密钥 μ 的变化敏感度测试

通过对算法的密钥空间和密钥敏感度进行分析发现，算法具有较大的密钥空间和较强的密钥敏感度，因此可以预见所提算法具有一定的应用前景。

结束语　本文在 MPEG 音频压缩的背景下提出了一种基于混沌和小波变换的音频信号加密算法，避免了因音频信号中存在特殊的语音、语调或长时间的停顿而被有经验的攻击者通过推测判断进行篡改，从而威胁到音频数据的安全。

经所提算法加密后的音频具有直方图分布均匀对称、邻域相关度小、密钥空间较大和密钥敏感度较强等优点，因此能够维护用户语音隐私和保证音频在互联网上安全传输。

参 考 文 献

[1] SADKHAN S B, AL-SHERBAZ A, MOHAMMED R S. Chaos based cryptography for voice encryption in wireless communication[C]// 2013 International Conference on Electrical, Communication, Computer, Power, and Control Engineering (ICECCPCE). IEEE, 2013: 191-197.

[2] GANESAN K, MUTHUKUMAR R, MURALI K. Look-up Table Based Chaotic Encryption of Audio Files[C]// IEEE Asia Pacific Conference on Circuits and Systems, 2006 (APCCAS 2006). IEEE, 2006: 1951-1954.

[3] ELSHAMY E M, EL-RABAIE E S M, FARAGALLAH O S, et al. Efficient audio cryptosystem based on chaotic maps and double random phase encoding [J]. International Journal of Speech Technology, 2015, 18(4): 619-631.

[4] WANG X, GUO K. A new image alternate encryption algorithm based on chaotic map[J]. Nonlinear Dynamics, 2014, 76(4): 1943-1950.

[5] FARAGALLAH O S. Efficient confusion-diffusion chaotic image cryptosystem using enhanced standard map[J]. Signal Image & Video Processing, 2015, 9(8): 1-10.

[6] PHILLIPS V J, LEE M H, THOMAS J E. Speech scrambling by the re-ordering of amplitude samples[J]. Radio & Electronic Engineer, 1971, 41(3): 99-112.

[7] JAYANT N S, COX R V, MCDERMOTT B J, et al. Analog Scramblers for Speech Based on Sequential Permutations in Time and Frequency[J]. Bell System Technical Journal, 1983, 62(1): 25-46.

[8] LIU J, GAO F, MA H. A Speech Chaotic Encryption Algorithm Based on Network[C]// International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2008 (IIHMSP'08). IEEE, 2008: 283-286.

[9] 吴乐南. 数据压缩的原理与应用[M]. 北京：电子工业出版社，1995(2)：33-37.

[10] 吴家安. 数据压缩技术及应用[M]. 北京：科学出版社，2009.

[11] BRANDENBURG K, STOLL G. ISO/MPEG-1 Audio: A Generic Standard for Coding of High-Quality Digital Audio[J]. Journal of Audio Engineering Society, 1994, 42(10): 780-792.

[12] LIU L P, ZHANG X F. Image encryption algorithm based on chaos and bit operations[J]. Journal of Computer Applications, 2013, 33(4): 1070-1073. (in Chinese)
刘乐鹏，张雪锋. 基于混沌和位运算的图像加密算法[J]. 计算机应用，2013，33(4)：1070-1073.

[13] FAN J L, ZHANG X F. Piecewise Logistic Chaotic Map and Its Performance Analysis[J]. Acta Electronica Sinica, 2009, 37(4): 720-725. (in Chinese)
范九伦，张雪锋. 分段 Logistic 混沌映射及其性能分析[J]. 电子学报，2009，37(4)：720-725.

[14] GROSSMANN A, MORLET J. Decomposition of Hardy functions into square integrable wavelets of constant shape[J]. Siam Journal on Mathematical Analysis, 1984, 15(4): 723-736.

[15] DAUBECHIES I. Ten Lectures on Wavelets[J]. Computers in Physics, 1992, 6(3): 1671-1671.

[16] MALLAT S G. A Theory for Multiresolution Signal Decomposition: The Wavelet Representation[J]. IEEE Transactions on Pattern Analysis & Machine Intelligence, 1989, 11(7): 674-693.

[17] XU K, XU J W, BAN X J. Foreacasting of Some Non-Stationary Time Series Based on Wavelet Decomposition[J]. Acta Electronica Sinica, 2001, 29(4): 566-568. (in Chinese)
徐科，徐金梧，班晓娟. 基于小波分解的某些非平稳时间序列预测方法[J]. 电子学报，2001，29(4)：566-568.

[18] 廉士国. 多媒体快速加密算法研究[D]. 南京：南京理工大学，2005：19-20.

[19] SRIDHARAN S, DAWSON E, GOLDBURG B M. Speech encryption using discrete orthogonal transforms[C]// International Conference on Acoustics, Speech, & Signal Processing. IEEE, 1990: 1647-1650.

[20] 刘东东. 提升移动话音质量(MOS)相关技术研究[D]. 北京：北京邮电大学，2012.

[21] SEYEDZADEH S M, MOOSAVI S M S, MIRZAKUCHAKI S. Using self-adaptive coupled piecewise nonlinear chaotic map for color image encryption scheme[C]// 2011 19th Iranian Conference on Electrical Engineering (ICEE). IEEE, 2011: 1-6.

[22] DU R S, SHANG F H, LI Y. Application of compound chaotic mapping in speech encryption algorithm[J]. Computer Engineering and Applications, 2009, 45(7): 103-104. (in Chinese)
杜睿山，尚福华，李阳. 复合混沌映射在语音加密算法中的应用[J]. 计算机工程与应用，2009，45(7)：103-104.