



# 基于 QR 分解和提升小波变换的鲁棒音频水印方法

马晓红\*, 赵琳琳

(大连理工大学信息与通信工程学院, 辽宁大连 116024)

**摘要:** 利用 QR 分解的稳定性以及提升小波计算速度快的优良特性, 给出一种基于 QR 分解和提升小波变换的盲鲁棒数字音频水印方法. 为了保护原始二值水印图像的安全, 利用混沌序列对其进行扩频, 生成了待嵌入的水印信号. 将原始宿主音频信号升维后进行 QR 分解, 根据  $R$  分量是上三角矩阵且第一行为非零元素的特点, 选定  $R$  分量的第一行, 对其进行提升小波变换, 得到了待嵌入的小波系数, 利用线性瞬时混合模型将其与待嵌入的水印信号进行混合, 得到隐秘音频信号. 水印提取时, 利用独立分量分析算法从待检测的隐秘音频信号中提取嵌入水印信号, 获得嵌入水印信号的估计, 经过后处理即可获得水印图像. 实验结果表明, 该方法可以实现水印的盲提取, 并且具有良好的透明性和鲁棒性.

**关键词:** 鲁棒水印; 提升小波变换; QR 分解; 独立分量分析

**中图分类号:** TP391 **文献标志码:** A

## 0 引言

随着网络规模的不断扩大和数字化技术的不断成熟, 数字多媒体产品得到了广泛应用. 以 MP3 为代表的音乐制品变得更易传播, 从而促进了信息的共享, 并进一步推动了数字音乐作品的发展. 与此同时, 对版权保护也提出了新的挑战. 由于数字音频信息极易被无限制地任意编辑、复制与散布, 如何有效地保护版权及发行公司的合法权益成为人们日益关注的问题. 传统加密技术只能提供小范围的保护, 且具有安全性不足和流通性较差等弱点. 数字音频水印技术通过将代表作者信息的图像、签名或者是作品的序列号等信息嵌入到音乐制品中, 实现了版权保护的目[1,2].

现有的数字音频水印方法大致可以分为时域方法和变换域方法两大类. 前者通过修改宿主音频信号的时域采样值而嵌入水印, 典型的有最低有效位(LSB)法[3]和回声掩蔽法[4]等. 该方法一般具有可嵌入水印容量较小、抗攻击能力较差等弱点. 变换域方法通过修改宿主音频信号的变换域系数进行水印嵌入, 常用的变换有离散傅里

叶变换(DFT)[5]、离散余弦变换(DCT)和离散小波变换(DWT)等[6]. 该方法具有水印能量可以分布至所有音频样本, 能够充分利用人类听觉特性, 且与数据压缩标准兼容等优点, 因而具有良好的鲁棒性, 已经成为研究与应用的热点. 小波提升法[7,8]由 Sweldens 等提出, 该方法不依赖于傅里叶变换, 可以直接在时空域中完成小波变换, 具有算法简单、计算速度快等优良特性, 在数字水印领域得到了广泛应用[9].

本文给出一种基于 QR 分解和提升小波变换的鲁棒音频水印方法. 该方法将原始宿主音频信号升维后进行 QR 分解, 对其  $R$  分量第一行进行提升小波变换, 得到待嵌入的小波系数, 利用线性瞬时混合模型将其与待嵌入的水印信号进行混合, 得到隐秘音频信号. 水印提取时, 利用独立分量分析算法提取嵌入水印信号, 获得嵌入水印信号的估计, 经过后处理即可获得水印图像.

## 1 基本理论

### 1.1 QR 分解

QR 分解[10]是一种线性代数工具. 任意一个

矩阵  $A \in R^{m \times n} (m \geq n)$  的 QR 分解可以表示为

$$A = Q \begin{pmatrix} R_1 \\ 0 \end{pmatrix} = QR \quad (1)$$

其中  $R_1$  为对角元大于零的上三角矩阵,  $Q$  为正交矩阵. 由于  $cond_2(A) = cond_2(R)$ , 即矩阵  $A$  和矩阵  $R$  的 2- 条件数相等, QR 分解具有数值稳定性.

### 1.2 提升小波变换

提升小波变换<sup>[11]</sup>的基本思想是基于欧几里德算法, 将小波变换分解成提升的形式, 并通过每一步提升所产生的浮点数取整, 实现整型变换. 小波提升过程如图 1 所示, 它包括分裂(split)、预测(predict)和更新(update)3 个步骤. 图 1 中 S 表示分裂, P 表示预测, U 表示更新.

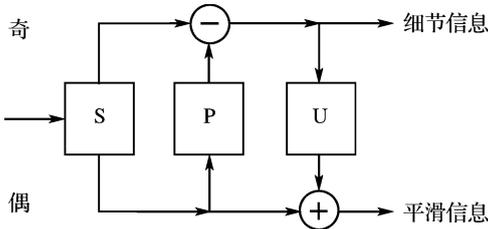


图 1 小波提升过程

Fig.1 The wavelet lifting procedure

### 1.3 独立分量分析

盲源分离用于解决在源向量和混合矩阵均为未知的情况下, 从观测向量中恢复出每个相互独立的源向量的问题. 假设有  $N$  个独立的源信号  $s_1, s_2, \dots, s_N$  和  $M$  个由这些源信号混合而成的观测信号  $x_1, x_2, \dots, x_M (M \geq N)$ , 盲源分离线性瞬时混合模型可以由下式表示:

$$x = As \quad (2)$$

式中:  $s = (s_1 \ s_2 \ \dots \ s_N)^T$ , 为源信号向量;  $x = (x_1 \ x_2 \ \dots \ x_M)^T$ , 为观测信号向量;  $A$  为混合矩阵.

信号经过变换后, 使不同信号分量之间的相依性最小化, 这种方法称为独立分量分析<sup>[12]</sup>算法, 它是解决盲源分离问题的一种比较成熟的方法.

## 2 基于 QR 分解和提升小波变换的鲁棒音频水印方法

基于 QR 分解和提升小波变换的鲁棒音频水印方法嵌入原理框图如图 2 所示. 它由嵌入水印信号生成、小波系数选取和水印信号的嵌入 3 个模块组成.

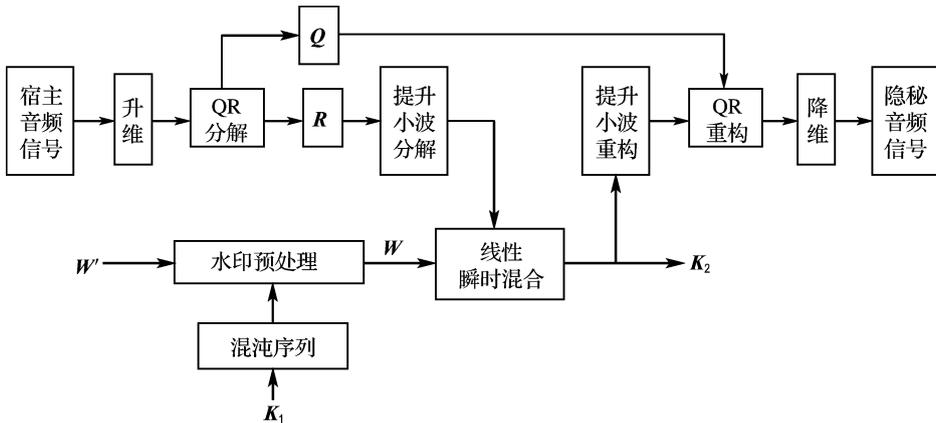


图 2 水印嵌入原理框图

Fig.2 The block diagram of watermark embedding

### 2.1 嵌入水印信号生成

为了保护原始二值水印图像的安全, 本文采用混沌序列<sup>[13]</sup>对其进行扩频处理.

混沌现象是在非线性动力系统中出现的确定性的和类似随机的过程, 这种过程既非周期又不收敛. 一类非常简单却被广泛研究的动力系统是 Logistic 映射, 其定义如下:

$$c_{k+1} = \mu c_k (1 - c_k); c_k \in (0, 1), 0 \leq \mu \leq 4 \quad (3)$$

式中:  $\mu$  为控制参数;  $c_0$  为初值. 当混沌映射参数满足  $3.569\ 945\ 6 < \mu \leq 4$  时, 该映射工作于混沌状态. 混沌序列具有对参数  $c_0$  和  $\mu$  敏感的特点.

设原始二值水印图像为  $W' = \{w'(m, n), 0 \leq m \leq M - 1, 0 \leq n \leq N - 1\}$ , 其中  $w'(m, n)$

表示图像中第  $m$  行、第  $n$  列像素的灰度值,  $M$  和  $N$  分别为水印图像的行数和列数. 嵌入水印信号的生成过程如下: 首先, 将原始水印图像降维成一维序列, 并将其元素的值映射为  $\{1, -1\}$  序列; 然后, 利用式 (3) 生成一个与该序列等长的混沌序列, 以 0.5 为阈值将其映射为一个  $\{1, -1\}$  序列; 对降维后的图像序列利用扩频技术进行加密处理, 即可生成待嵌入的水印信号  $\mathbf{W} = \{w(k), 0 \leq k \leq M \times N - 1\}$ . 生成混沌序列的初值作为密钥  $\mathbf{K}_1$  保留.

## 2.2 小波系数选取

考虑到 QR 分解具有良好的稳定性, 本文将原始宿主音频信号升维后进行 QR 分解, 根据  $\mathbf{R}$  分量是上三角矩阵且第一行为非零元素的特点, 选定  $\mathbf{R}$  分量的第一行, 对其进行提升小波变换, 得到了待嵌入的小波系数, 利用线性瞬时混合模型进行水印嵌入. 具体过程如下:

首先, 将一维原始宿主音频信号  $\mathbf{X}' = \{x'(n), 0 \leq n \leq L - 1\}$  升维为二维信号  $\mathbf{X}$ , 即  $\mathbf{X} = \{x(i, j), 0 \leq i \leq \frac{L}{M \times N} - 1, 0 \leq j \leq M \times N - 1\}$ . 其次, 对  $\mathbf{X}$  进行 QR 分解, 即  $\mathbf{X} = \mathbf{QR}$ , 其中  $\mathbf{Q}$  是正交矩阵,  $\mathbf{R}$  是上三角矩阵, 选择  $\mathbf{R}$  的第一行元素作为  $\mathbf{s}$ , 即  $\mathbf{s} = \{\mathbf{R}(1, j), 0 \leq j \leq M \times N - 1\}$ . 最后, 对  $\mathbf{s}$  进行提升小波变换, 得到待嵌入水印的小波系数.

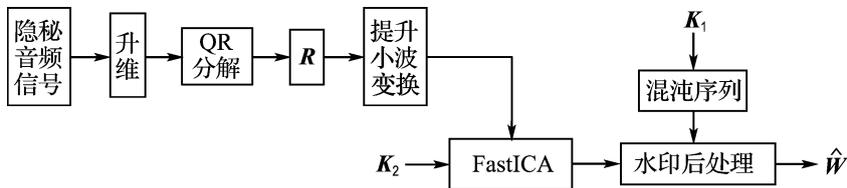


图3 水印提取原理框图

Fig. 3 The block diagram of watermark extracting

对待检测的隐秘音频信号升维后进行 QR 分解, 对  $\mathbf{R}$  矩阵的第一行元素进行提升小波变换, 将获得的小波系数和密钥  $\mathbf{K}_2$  作为两路源信号, 利用 FastICA 算法<sup>[14]</sup> 对其进行分离, 获得两路信号  $\mathbf{S}'_1$  和  $\mathbf{S}'_2$ , 分别计算它们的四阶统计量值, 值较小的一路信号即为分离出的水印信号  $\mathbf{w}'$ . 将  $\mathbf{w}'$  中的每一个元素以零为阈值进行二值化处理, 获得由  $-1$  和  $1$  构成的序列, 利用密钥  $\mathbf{K}_1$  对其进行混沌

## 2.3 水印信号的嵌入

将选定的小波系数  $\mathbf{s}$  和待嵌入的水印信号  $\mathbf{W}$  利用线性瞬时混合方法进行水印嵌入, 嵌入过程如下式所示:

$$\mathbf{S} = \begin{pmatrix} \mathbf{S}_1 \\ \mathbf{S}_2 \end{pmatrix} = \mathbf{A} \times \begin{pmatrix} \mathbf{s} \\ \mathbf{W} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \times \begin{pmatrix} \mathbf{s} \\ \mathbf{W} \end{pmatrix} \quad (4)$$

其中  $\mathbf{A}$  为满秩的混合矩阵, 为了保证隐秘音频信号的透明性, 其元素应满足条件  $a_{11} \gg a_{12}, a_{21} \gg a_{22}$ . 将第一路信号  $\mathbf{S}_1$  进行提升小波重构和 QR 重构, 并进行降维操作, 获得最终的隐秘音频信号. 另一路信号  $\mathbf{S}_2$  作为密钥  $\mathbf{K}_2$  保留, 以便进行水印信号提取.

这里之所以选择线性瞬时混合方法进行水印的嵌入, 主要原因在于: 不借助于密钥  $\mathbf{K}_2$  的帮助, 由隐秘音频信号是无法获得水印信号的, 因为这属于盲源分离问题中的欠定分离情况, 因此本文的水印方案具有很强的安全性. 但是, 该种嵌印方法也存在一个问题, 即需要保留的密钥数据量较大, 不利于密钥的管理. 可以将密钥升维成二维矩阵, 通过对其进行奇异值分解, 达到减少密钥数据量的目的.

## 3 水印图像的提取

水印提取过程是水印嵌入的逆过程, 其原理框图如图 3 所示.

逆映射, 进而转换为由 0 和 255 构成的二值序列, 升维后即可得到提取出的水印图像  $\hat{\mathbf{W}} = \{\hat{w}(m, n), 0 \leq m \leq M - 1, 0 \leq n \leq N - 1\}$ .

## 4 实验结果

为了验证本文方法的有效性, 分别选取语音信号、流行音乐、经典音乐和爵士乐等作为宿主信号. 下面以语音信号作为宿主信号为例, 给出相应

的实验结果.

宿主信号为一段采样率为 8 kHz, 长度为 65 536 点的语音信号, 实验中使用的各个参数值设置如下:  $M = N = 32$ ,  $a_{11} = 0.97$ ,  $a_{12} = 0.03$ ,  $a_{21} = 0.92$ ,  $a_{22} = 0.08$ .

#### 4.1 透明性测试

宿主语音信号和隐秘语音信号的时域波形图分别如图 4(a) 和 (b) 所示. 由图 4 可以看出, 二者在波形上几乎没有任何差别; 听音测试也表明, 二者在听觉质量上几乎没有任何差别, 表现出了良好的透明性.

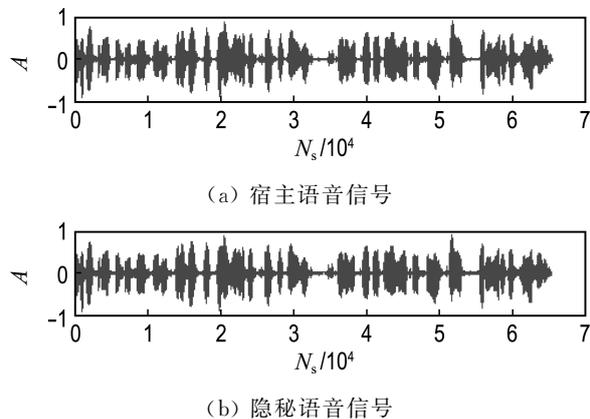


图 4 语音信号时域波形图

Fig. 4 The time domain waveform of speech signal

#### 4.2 安全性测试

图 5(a) 为原始二值水印图像, 图 5(b) 和 (c) 分别表示在密钥正确和错误 (误差为 1%) 情况下提取出的水印图像.

由图 5(c) 可以看出, 即使密钥发生微小变化, 也不能正确提取出水印图像, 因此水印图像的安全性可以由密钥信息来保证.



图 5 安全性测试

Fig. 5 The security testing

#### 4.3 鲁棒性测试

图 6 给出了隐秘语音信号在经过诸如 MP3、剪切、上采样、下采样、添加高斯白噪声、低通滤波、高通滤波等各种信号处理操作后提取出的水印图像.

由图 6(a) 和 (b) 可以看出, 本文方法可以有效地抵抗 MP3 攻击, 并具有较好的抗剪切攻击能力; 对比图 6(c) 和 (d) 可知, 下采样攻击比上采样攻击对鲁棒水印的影响大; 由图 6(f) 和 (g) 可知, 高通滤波比低通滤波对鲁棒水印造成的影响大; 由图 6(e) 可知, 添加 20 dB 的高斯白噪声, 会引起鲁棒水印轻微的降质.



图 6 隐秘信号经过常规信号处理攻击后提取出的水印图像

Fig. 6 Extracted watermark images from watermarked signal under common signal processing attacks

## 5 结 论

本文给出了一种基于 QR 分解和提升小波变换的鲁棒数字音频水印方法. 该方法充分利用了 QR 分解的稳定性, 以及提升小波变换的快速性等良好特性. 采用线性瞬时混合方法实现了水印的嵌入, 利用 FastICA 算法实现了水印的盲提取. 实验结果表明, 该方法具有良好的安全性、透明性和鲁棒性.

## 参考文献:

- [1] 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
- [2] LIE W N, CHANG L C. Robust and high-quality time-domain audio watermarking based on low-frequency amplitude modification [J]. *IEEE Transactions on Multimedia*, 2006, 8(1):46-59
- [3] CERZON M A, GRAVEN P G. A high rate buried data channel for audio CD [J]. *Journal of Audio*

- Engineering Society**, 1995, **43**(1-2):3-22
- [4] KIM H J, CHOI Y H. A novel echo-hiding scheme with backward and forward kernels [J]. **IEEE Transactions on Circuits and Systems for Video Technology**, 2003, **13**(8):885-889
- [5] LU C S, LIAO H Y M, CHEN L H. Multipurpose audio watermarking [C] // **IEEE International Conference on Pattern Recognition**. Washington D C: IEEE Computer Society, 2000:282-285
- [6] WANG X Y, ZHAO H. A novel synchronization invariant audio watermarking scheme based on DWT and DCT [J]. **IEEE Transactions on Signal Processing**, 2006, **54**(12):4835-4840
- [7] CLAYPOOLE R L, DAVIS G M, SWELDENS W, *et al.* Nonlinear wavelet transforms for image coding via lifting [J]. **IEEE Transactions on Image Processing**, 2003, **12**(12):1449-1459
- [8] CALDERBANK A R, DAUBECHIES I, SWELDENS W, *et al.* Lossless image compression using integer to integer wavelet transforms [C] // **International Conference on Image Processing**. Washington D C:IEEE Signal Processing Society, 1997:596-599
- [9] 王让定,徐达文. 基于提升小波的多重数字音频水印 [J]. 电子与信息学报, 2006, **28**(10):1820-1826
- [10] 施吉林,张宏伟,金光日. 计算机科学计算 [M]. 北京:高等教育出版社, 2005:33-36
- [11] SALOMON D. 数据压缩原理与应用 [M]. 吴乐南,等译. 北京:电子工业出版社, 2003:393-395
- [12] COMON P. Independent component analysis:a new concept [J]. **Signal Processing**, 1994, **36**(3):287-314
- [13] 张志明,王 磊. 基于混沌加密的 DCT 域图像水印算法 [J]. 计算机工程, 2003, **29**(17):9-10
- [14] HYVARINEN A. Fast and robust fixed-point algorithms for independent component analysis [J]. **IEEE Transactions on Neural Networks**, 1999, **10**(3):626-634

## A robust audio watermarking method based on QR decomposition and lifting wavelet transform

MA Xiao-hong\*, ZHAO Lin-lin

( School of Information and Communication Engineering, Dalian University of Technology, Dalian 116024, China )

**Abstract:** Making use of the good stability of QR decomposition and good computing ability of lifting wavelet, a blind robust digital audio watermarking method based on QR decomposition and lifting wavelet transform is proposed. To protect the security of the original binary watermarking image, chaotic sequence is used to spread its spectrum and watermarking signal for embedding is generated. In the watermark embedding procedure, first, QR decomposition is executed after rising dimension of the original host audio signal; then, as **R** component is an upside-triangle matrix and the element in its first row is nonzero, lifting wavelet transform is taken on its first row to obtain the selected wavelet coefficients; last, the watermarking signal is embeded into the selected wavelet coefficients using linear instantaneous mixing model to generate the watermarked audio signal. In the watermark extraction procedure, independent component analysis algorithm is utilized to extract the watermarking signal from the watermarked audio signal for detecting. The watermarking image can be obtained after post-processing. Experimental results show that this method can achieve blind extraction of watermark and has good transparency and robustness.

**Key words:** robust watermark; lifting wavelet transform; QR decomposition; independent component analysis