

一种均匀量化小波能量的盲提取音频水印算法

马德洋¹, 卢 忱², 范九伦¹

(1 西安邮电大学 通信与信息工程学院, 陕西 西安 710061; 2 武警工程大学 通信工程系, 陕西 西安 710086)

摘 要: 为了更好的保护版权并保证隐藏通信, 建立了嵌入同一个水印并通过不同的密钥来分别得到鲁棒水印和脆弱性水印的模型, 基于此提出了采用双极性量化策略对离散小波高频系数总能量进行均匀量化的盲提取音频水印算法. 新算法以水印的特征值作为水印预处理的密钥. 仿真实验表明该方案具备较好的鲁棒性和脆弱性.

关键词: 盲提取音频水印; 离散小波变换; 均匀量化; 鲁棒性; 脆弱性

中图分类号: TP309

文献标识码: A

文章编号: 1000-7180(2013)03-0043-04

An Algorithm of Blind Extracting Audio Watermarking Based on Wavelet Energy with Uniform Quantization

MA De-yang¹, LU Chen², FAN Jiu-lun¹

(1 School of Communication and Information Engineering, Xi'an University of Posts and Telecommunications, Xi'an 710061, China; 2 Department of Communication Engineering, Armed Police Engineering University, Xi'an 710086, China)

Abstract: In order to protect the copyright and guarantee the hidden communication better, the model which can get robust and fragile watermarks with the same embedded watermark through the different keys is established. And then the blind extracting audio discrete watermarking algorithm based on polarity quantification of uniform quantitative the high frequency of total wavelet energy is proposed. The new algorithm takes the characteristic value of the watermark as the key of watermark pretreatment. Experimental result shows that the project has better robustness and fragility.

Key words: blind extracting audio watermarking; discrete wavelet transform; uniform quantization; robustness; fragility

1 引言

数字水印技术是为了在图像、音频、视频等多媒体中隐藏秘密信息而产生的一种技术^[1], 而音频水印算法研究相对较少^[2]. 随着微信、飞聊等语音业务的流行, 作为既能保护版权又能在其中隐藏机密信息的音频水印受到越来越多的关注.

数字水印可分为两个层面, 一种是为了实现版权保护, 另一种是为了隐藏信息. 为了使得嵌入的水印同时具备这两种性能, 研究者们进行了一些探讨^[3], 但大多是加入两种水印, 这使得原载体承载了

双倍的水印信息. 鉴于此, 本文针对音频数字水印, 提出只嵌入一个水印, 通过不同的密钥来分别实现这两种功能的方法.

2 水印预处理

二值水印可采用一定的算法来提取特征值 K . 本文采用对二值水印矩阵 B 求和的方式提取(可以采用其它安全性高的算法, 如求哈希值)特征值, 其中 Arnold 置乱的周期为 N :

$$K = \text{mod}(\text{sum}(B), N)$$

收稿日期: 2012-06-12; 修回日期: 2012-07-10

基金项目: 陕西省科技统筹创新工程计划项目(2011KTCQ01-23)

2.1 Arnold 置乱

Arnold 变换是基于遍历理论提出的一种裁剪变换. 根据式(1)对图像的像素点位置进行变换, 从而达到对图像置乱的效果. 本文对水印进行 K 次 Arnold 置乱, 然后将其降为一维二值序列 W .

假设嵌入到音频信号 A 中的二值水印图像表示为: $B = (b(i, j); 0 \leq i, j \leq m)$. 对水印图像使用 Arnold 变换置乱之后的坐标为 $b(i', j')$. 变换公式为:

$$\begin{bmatrix} i' \\ j' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} i \\ j \end{bmatrix} \bmod m \quad (1)$$

2.2 混沌加密

引入混沌理论^[4]以 K 为密钥, 采用一定算法生成 α, β (本文采用 $\alpha = \text{mod}(K, \pi), \beta = K - \alpha\pi$), 进一步利用迭代算法生成 0、1 混沌序列 M . Arnold 置乱之后的水印矩阵 B' 降维生成二值序列 W , 计算要嵌入的水印序列

$$W = w \oplus M \quad (2)$$

3 水印嵌入算法

(1) 对音频信号 A 进行 3 次小波变换, 得到近似

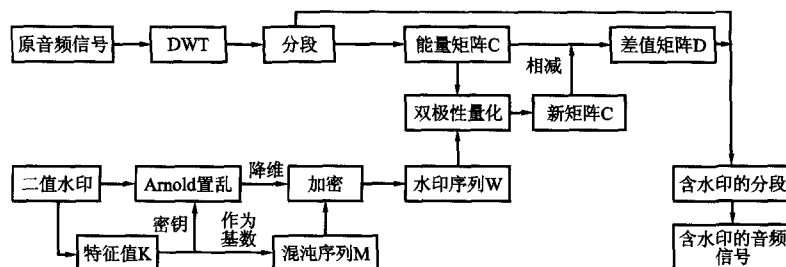


图1 水印嵌入算法框图

3.1 双极性量化

对能量矩阵 $C(\alpha) \{0 \leq \alpha \leq L\}$ 对应水印序列 W 进行双极性量化. 待量化系数为 f , 量化后系数为 f' , 量化步长为 Δ , 量化原理图如图 2 所示. 量化步长 Δ 采用自适应算法:

$$\Delta = q \times (E_a / E_{sum}) \quad (3)$$

其中 q 为基准步长, E_a 为嵌入点附近 n 个点的能量和, E_{sum} 为参与量化的总能量. Δ 选取越小, 水印透明性越好; Δ 选取越大, 水印鲁棒性越好.

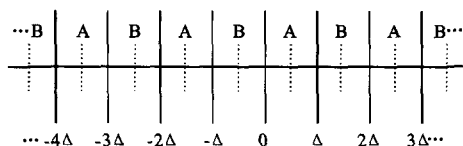


图2 双极性量化原理

将能量矩阵 c 按照水印序列 w 进行量化. 当 $w(i)$ 为 0 时, 将系数 f 量化为 A 区间的中间值; 当为

分量 $ca1, ca2, ca3$, 细节分量 $cd1, cd2, cd3$.

(2) 将 $ca3$ 对应水印序列 W 中元素的个数 L 平均分为 L 段. L 段分量中, 每个分量含 m 个小波系数, 记为 $S_\alpha(i), (0 \leq \alpha \leq L, 0 \leq i \leq m)$.

(3) 对每段分量求和得到含 L 个值的能量矩阵 $C(\alpha) (0 \leq \alpha \leq L)$, 即 $C(\alpha) = \sum_{i=0}^m S_\alpha(i)$.

(4) 能量矩阵 c 按照水印序列 W 进行双极性均匀量化, 量化之后的矩阵为 $C(\alpha)$.

(5) c' 与 c 相减得到差值矩阵 $D(\alpha)$.

(6) D 中元素值 $D(\alpha)$ 依次平均加入到 S_α 中, 即 $S_\alpha(i) = \frac{D(\alpha)}{m}$. 从而得到含水印信息的分段.

将分段进行小波逆变换重构音频信号, 整个水印嵌入算法结束 (分段时音频中多余的部分不进行处理). 水印嵌入算法流程如图 1 所示.

1 时, 将系数 f 量化为 B 区间的中间值.

(1) 判断 f 在 A, B 哪个区间. 这里小波系数大多为小数, 牵扯到精确度的问题使得取模运算不精确, 所以采用下面算法; 这里 m 为模值, r 为余数.

$$m = \text{floor}(f/\Delta) \quad (4)$$

$$r = f - m \times \Delta \quad (f \geq 0 \text{ 时})$$

$$m = -\text{floor}(\text{abs}(f/\Delta)) \quad (5)$$

$$r = f - m \times \Delta \quad (f < 0 \text{ 时})$$

(2) 根据 W 对 f 进行量化处理, 处理算法如下:

当 $f \geq 0$ 且 $W(i) = 0$ 时,

$$f' = \begin{cases} m\Delta + \frac{1}{2}\Delta, & m = 2k \\ (m-1)\Delta + \frac{1}{2}\Delta, & m = 2k, |r| < \frac{1}{2}\Delta \\ (m+1)\Delta + \frac{1}{2}\Delta, & m = 2k, |r| > \frac{1}{2}\Delta \end{cases} \quad (6)$$

当 $f \geq 0$ 且 $W(i) = 1$ 时,

$$f' = \begin{cases} m\Delta + \frac{1}{2}\Delta, & m = 2k+1 \\ (m-1)\Delta + \frac{1}{2}\Delta, & m = 2k, |r| < \frac{1}{2}\Delta \\ (m+1)\Delta + \frac{1}{2}\Delta, & m = 2k, |r| > \frac{1}{2}\Delta \end{cases} \quad (7)$$

当 $f < 0$ 且 $W(i) = 0$ 时,

$$f' = \begin{cases} m\Delta - \frac{1}{2}\Delta, & m = -(2k+1) \\ (m+1)\Delta - \frac{1}{2}\Delta, & m = -2k, |r| < \frac{1}{2}\Delta \\ (m-1)\Delta - \frac{1}{2}\Delta, & m = -2k, |r| > \frac{1}{2}\Delta \end{cases} \quad (8)$$

当 $f < 0$ 且 $W(i) = 1$ 时,

$$f' = \begin{cases} m\Delta - \frac{1}{2}\Delta, & m = -2k \\ (m+1)\Delta - \frac{1}{2}\Delta, & m = -(2k+1), |r| < \frac{1}{2}\Delta \\ (m-1)\Delta - \frac{1}{2}\Delta, & m = -(2k+1), |r| > \frac{1}{2}\Delta \end{cases} \quad (9)$$

通过以上算法将水印信息嵌入到矩阵 c 中, f 到 f' 量化产生的误差最大为 Δ 。

3.2 水印嵌入后处理及重构音频信号

此时 c 中已经含有水印信息,与能量矩阵相减得到差值矩阵 $D(a)$, $\{0 \leq a \leq L\}$,将 D 中元素依次平均加入到 L 个原小波变化系数分段中,进行小波逆变化重构得到含有水印的音频信号。

4 提取水印算法

(1)对待提取水印音频信号进行相应次小波变化。

(2)取近似分量,分成 L 段,每段含 m 个元素。

(3)每段各自求和重组能量矩阵 $E(i)$ $\{0 \leq i < L\}$ 。

(4)对 E 中元素依次判读所属分区,提取水印:

若 $E(i) \in A$,则水印 $w = 0$;

若 $E(i) \in B$,则水印 $w = 1$ 。

(5)混沌解密,并升维。

(6)Arnold 置乱还原。

提取水印过程不依赖原始音频信号实现了盲提取。

4.1 鲁棒水印提取

使用原水印图像的特征值作为密钥进行提取,可以得到鲁棒水印,流程如图3所示。

4.2 脆弱性水印提取

使用提取水印信息的特征值作为密钥进行提取,可以得到脆弱性水印,流程如图4所示。

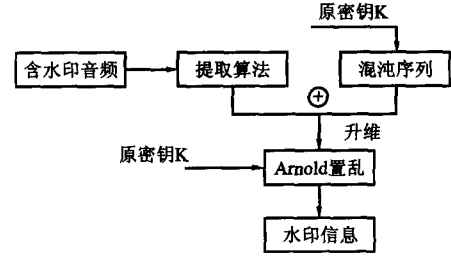


图3 水印提取方法(鲁棒水印)

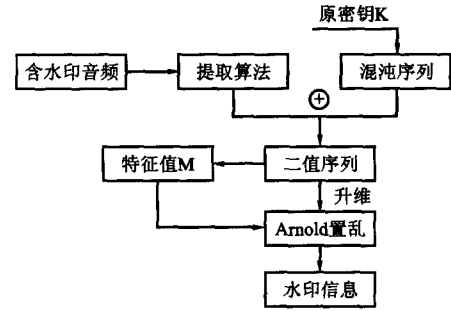


图4 水印提取方法(脆弱性水印)

4.3 快速检验载体信号是否受攻击

本文方案能快速检验信号是否受攻击,流程如图5所示。

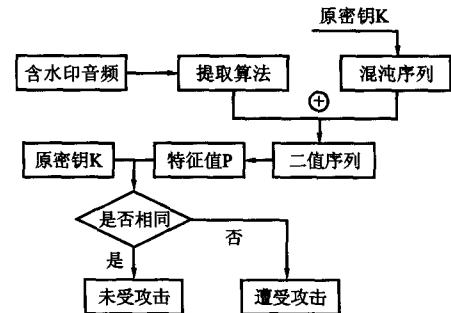


图5 检测是否受攻击方法

5 实验仿真及结果分析

原始音频信号为单声道、8kHz、8位 WAV 文件. 水印信息是一幅内容为“西部通工” 32×32 的二值图像. 特征值提取采用 $K = \text{mod}(\text{sum}(B), N)$ 算法, K 作为 Arnold 置乱的次数,并且作为混沌基数参与生成混沌序列,小波基取‘db1’. 图6为水印嵌入前后的音频信号图,嵌入前后音频信号听不出来区别^[5-6]。

实验仿真了几种常见攻击:

(1)添加高斯噪声:加入 43db 高斯噪声。

(2)对水印信号进行下采样,由原来的 8kHz 变为 5kHz。

(3)对水印的音频信号进行低通滤波,最大频率为 10kHz.

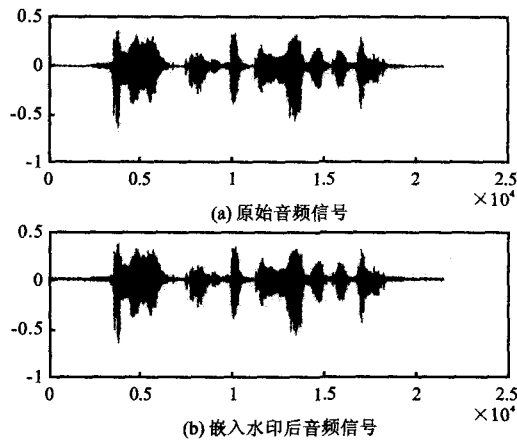


图 6 水印嵌入前后的音频信号图

实验所得加入水印前后的信噪比系数如表 1 所示.

表 1 各种攻击的信噪比

	未攻击	高斯攻击	下采样	低通滤波
SNR	48.834	37.851	48.357	38.113

实验结果表明,该算法能提取较好的鲁棒水印,具备保障隐藏通信的功能特性.

利用前面所述的方法提取相应的脆弱性水印.提取水印如图 7 所示.表明该算法对几种常见攻击有较好的脆弱性,能有效保障载体的完整性,具备保护版权功能特性.



图 7 提取脆弱性水印

6 结束语

文中提出均匀量化小波能量的盲提取水印算

法,并建立了提取不同水印的模型.仿真实验证明,该算法有较好的鲁棒性和脆弱性,同时具备了保护版权和实现隐藏信息的功能特性.其中涉及到的特征值提取算法和基于特征值的混沌基数生成算法等都过于简单,要进一步提高安全性,还有待更进一步的研究改进.

参考文献:

[1] 张荣跃,倪江群等.基于小波域 HMM 模型的稳健多比特图像水印算法[J].软件学报,2005,16(7):1323-1332.

[2] Huang Jiwu, Wang Yong, Shi Y Q. A blind audio watermarking algorithm with self-synchronization [C]// Proceedings of IEEE International Symposium on Circuits and Systems. Arizona, USA,2002(3):627-630

[3] 陆佰林,朱艳琴.基于小波变换的双水印算法[J].微电子学与计算机,2007,24(8):31-34.

[4] Li Ping, Li Zhong, Halanga W A, et al. A multiple pseudo and ambit generator based on a spatic temporal chaotic map [J]. Physics Letters A, 2006, 349(6): 467-473.

[5] 任洪娥,尚振伟,张健.一种基于 Arnold 变换的数字图像加密算法[J].光学技术,2009,35(3):384-387.

[6] Wang Xiangyang, Zhao Hong. A novel synchronization invariant audio watermarking scheme based on DWT and DCT [J]. IEEE transactions on signal processing, 2006, 54(12):4835-4840.

作者简介:

马德洋 (1988-),硕士研究生.研究方向为通信安全与信息对抗.

卢忱 (1965-),博士,副教授.研究方向为通信安全.

范九伦 (1964-),教授,博士生导师,CCF 高级会员.研究方向为模式识别、信息安全.