

基于奇异值分解与融合的音频盲认证算法^{*}

王 潇, 柏 森, 赵 波

(重庆通信学院, 重庆 400035)

摘 要: 提出一种适用于检验音频真实性和完整性的盲音频认证方法。它采用奇异值分解 (SVD) 与融合技术相结合, 将音频奇异值分解所得的奇异值作为不变特征, 利用融合将其嵌入到原始音频中。验证时无需原始音频数据, 利用融合的逆过程提取不变特征, 进行匹配, 达到音频认证的目的。实验结果表明, 该算法不但可以有效地检测出音频中被篡改内容的位置, 而且能将随机噪声同恶意篡改区分开。

关键词: 音频认证; 奇异值分解; 融合

中图分类号: TP391 **文献标识码:** A **文章编号:** 0529-6579 (2004) S2-0188-04

随着计算机技术的发展, 特别是海量存储设备和大容量内存在 PC 机上的实现, 对音频媒体进行数字化处理便成为可能。而音频的数字化处理使音频媒体极易被篡改, 破坏了音频媒体的真实性和完整性。在某些情况下, 需要进行基于目标音频的认证。譬如, 在法律诉讼过程中, 如果原告或者被告中的一方提供了一段已经被篡改的音频作为证据, 那么另一方就可以运用音频认证的方法证明该音频证据是不可靠的。

目前, 图像认证已成为信息认证领域的研究热点, 而对于音频认证的研究则相对较少。文献^[1]通过将原始音频的傅立叶系数量化来设计水印, 然后利用鸡尾酒水印算法嵌入水印。实现了对音频数据水印的嵌入及音频认证。^[2]中将掩蔽曲线作为音频的不变特征对音频进行认证。

本文提出基于奇异值分解^[3,4]和融合^[5]技术相结合的鲁棒盲音频认证算法。实验表明, 所提出的算法不但可以有效地检测出音频中被篡改内容的位置, 而且能将随机噪声同恶意篡改区分开。

1 奇异值分解 (SVD) 及其特性

有关奇异值分解的定理^[4]如下:

定理 1 矩阵的奇异值分解定义

$$A = P \begin{bmatrix} D & 0 \\ 0 & 0 \end{bmatrix} Q^H$$

其中 P, Q 为酉矩阵, $D = \text{diag} (d_1, d_2, \dots, d_r)$, 且 $d_1 \geq d_2 \geq \dots \geq d_r$ 是 A 的奇异值, 它是 AA^H 或 $A^H A$ 的

特征值的 λ_i 平方根。

定理 2 奇异值的稳定性

假设 $A, B \in C^{m \times n}$, A, B 的奇异值分别为 $d_1 \geq d_2 \geq \dots \geq d_r, \beta_1 \geq \beta_2 \geq \dots \geq \beta_r$, 则 $|d_i - \beta_i| \leq \|PA - BP\|_2$ 即矩阵有小的波动, 奇异值的变化不大于扰动矩阵的 2 范数。

奇异值的这种特性, 可以用来抑制噪声对音频数据的影响, 增强了音频认证算法的鲁棒性。

2 SVD 与融合相结合的音频认证算法

由于音频奇异值分解后, 其奇异值有良好的稳定性, 故我们将奇异值作为音频的不变特征。认证时根据不变特征的变化情况, 对音频文件的真实性和完整性作出判断。不变特征对整个音频认证过程至关重要, 因此要将其准确无误地传送到接收端。文献^[4]将不变特征作为标签附在要传送的图像之后, 这样做就会引起数据量的膨胀, 并且受到恶意攻击 (如标签被刻意删除) 时极有可能无法进行认证。本文将不变特征作为水印利用融合, 直接嵌入到原文件中就克服了上述问题, 实现了不变特征的盲提取, 并能进行篡改定位, 实验证明对随机噪声有很好的鲁棒性。整个过程如图 1 所示。

2.1 音频数据的预处理

目前, 奇异值分解在图像处理等方面应用广泛。而由于音频数据本身的特性: 它是连续的波。我们不能直接对它进行奇异值分解。因此, 必须先对音频数据进行适当的处理。

* 收稿日期: 2004-09-11

基金项目: 重庆市应用基础研究资助项目 (8028)

作者简介: 王潇 (1980 年生), 女, 硕士研究生; E-mail: wangxiaoyan_8882003@yahoo.com.cn

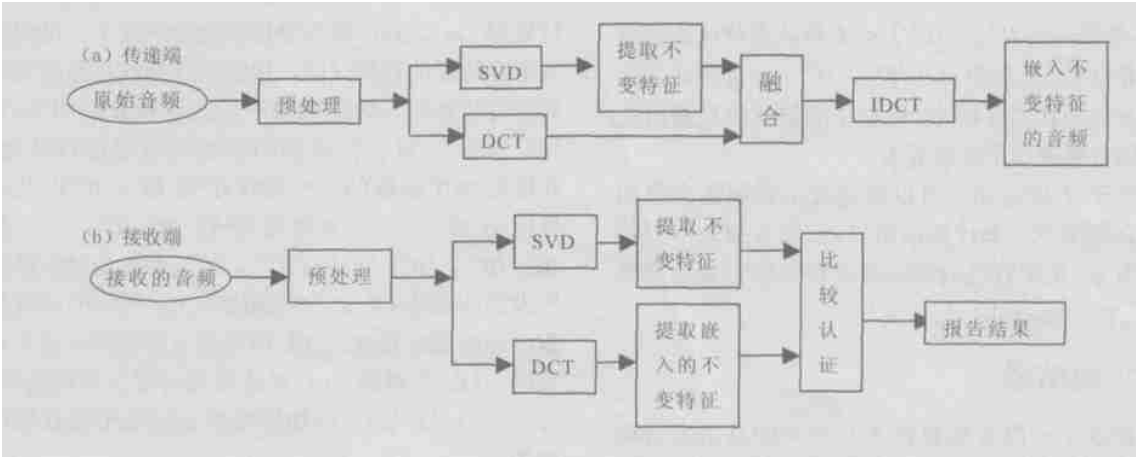


图 1 基于 SVD 和融合的盲音频认证流程图

Fig 1 The flow diagram for blind audio authentication based on SVD and amalgamation

首先, 对音频信号进行 A/D 转换, 得到数字化的数据, 我们把它记为矩阵 B 。采样频率的不同, B 的长度是不同的。本文中, 采样频率 $F=8\,000\text{ Hz}$, 得 $B=[b_1, b_2, \cdots, b_k]$ 。将 B 等分成长度为 $m\times m$ 的子矩阵 (不足的用零补齐), 得到 $B_1, B_2, \cdots, B_n$, 如下:

$$B = [b_1, b_2, \cdots, b_{m\times m}, b_{m^1+1}, \cdots, b_{m^2}, \cdots, \\ B_1 \qquad \qquad \qquad B_2 \\ b_{(n-1)\times m^2+1}, \cdots, b_k, 0, \cdots, 0] \\ B_n$$

再将 $B_1, B_2, \cdots, B_n$ 分别转换成 m 阶方阵 $E_1, E_2, \cdots, E_n$:

$$E_i = \begin{bmatrix} b_{1+(i-1)\times m^2} & b_{2+(i-1)\times m^2} & \cdots & b_{m+(i-1)\times m^2} \\ b_{m+1+(i-1)\times m^2} & b_{m+2+(i-1)\times m^2} & \cdots & b_{2m+(i-1)\times m^2} \\ \cdots & \cdots & \cdots & \cdots \\ b_{(m-1)\times m+1+(i-1)\times m^2} & b_{(m-1)\times m+2+(i-1)\times m^2} & \cdots & b_{m\times m+(i-1)\times m^2} \end{bmatrix} \\ (i=1, 2, \cdots, n)$$

2.2 音频数据的奇异值分解及不变特征的融合

在发送端, 经过上述预处理过程, 就可以对音频文件进行如图 1 所示的处理, 从而将不变特征嵌入到原始音频中。奇异值分解所得的奇异值矩阵, 其奇异值由大到小排列。正常操作 (引如噪声) 并不会对每个音频块较大奇异值产生大的影响, 因此可将其作为不变特征提取。主要步骤如下:

第一步: 由

$$E_i = P_i \begin{bmatrix} SE_i & 0 \\ 0 & 0 \end{bmatrix} Q_i^H, i=1, 2, \cdots, n$$

对 $E_1, E_2, \cdots, E_n$ 分别进行奇异值分解, 得到奇异值矩阵 SE_i 。将 SE_i 中较大的特征值提取出来, 得到不变特征 IF_i ;

设 $SE_i = \text{diag}(d_{i1}, d_{i2}, \cdots, d_m)$, 则
 $IF_i = (d_{i1}, d_{i2}, \cdots, d_f)$

其中, $f < m$

第二步: 对 $B_i(i=1, 2, \cdots, n)$ 进行离散余弦变换 (DCT), 得到 DB_i :

$$DB_i = (db_{i1}, db_{i2}, \cdots, db_{im^2})$$

第三步: 利用融合^[9]技术, 将 IF_i 融合到 DB_i 中, 得到 DB'_i :

$$\begin{cases} DB'_i = (db'_{i1}, db'_{i2}, \cdots, db'_{im^2}) \\ db'_{i(2f-1)} = db_{i(2f-1)} \\ db'_{i(2f)} = (1-t) \times db_{i(2f-1)} + t \times d'_{ij} \end{cases}$$

其中 $i=1, 2, \cdots, n, j=1, 2, \cdots, f, t \in [0, 1]$

第四步: 对 DB'_i 进行反离散余弦变换 (IDCT) 得到 B'_i , 依次将 B'_i 连接起来就得到融合了原始音频不变特征的音频 B' 。

由于 B' 是由 B 作一些极小的改动而得, 不会对 B 的听觉效果造成影响。因此我们将 B' 作为最终的音频文件进行传送或保存。

2.3 音频认证处理

对于待认证的音频材料 B'' , 主要采用如下的三个步骤进行认证:

第一步: 用 2.1 节介绍的方法对 B'' 作预处理, 得到相应的 E''_i 和 B''_i 。

第二步: 对 E''_i 奇异值分解并提取不变特征 IF'_i 。

第三步: 对 B''_i 进行离散余弦变换得到 $DB''_i = (db''_{i1}, db''_{i2}, \cdots, db''_{im^2})$, 提取不变特征 $IF''_i = (d''_{i1}, d''_{i2}, \cdots, d''_{if})$, 其中 $f < m$;

$$d''_{if} = [db''_{i(2f)} - (1-t) \times db''_{i(2f-1)}] / t$$

第四步: 根据门限值 T 对 $\text{abs}(IF'_i - IF''_i)$ 进行

判断,如果 $\text{abs}(IF'_i - IF''_i) < T$ 则认为待认证音频已被恶意篡改,如果 $\text{abs}(IF'_i - IF''_i) \geq T$ 则认为待认证音频是真实可靠的。根据 i 的值就能判断出是哪一段音频遭到了恶意篡改。

对于 T 的选定,可以通过确定音频能容忍的最严重的噪声,来计算阈值 T 。设原音频的不变特征值为 ψ ,所能容忍的最大受损音频的不变特征值为 ψ , $T = \max(\text{abs}(\psi - \psi))$ 。

3 实验结果

截取了一段音频数据来对本文的算法进行验证。如图 2 所示, (a) 为原始音频, 发送端对其进

行处理 ($m = 50$), 将不变特征融合进其中, 得到嵌入不变特征的音频 (b)。接收端收到的是恶意篡改后的音频和加入伪随机噪声后的音频分别用 (c)、(d) 表示。对它们分别用前述的方法进行处理, 获得经 DCT 提取的不变特征序列 IB' , IC' 以及奇异值分解后的不变特征序列 IB'' , IC'' 。(e) 为 $\text{abs}(IB' - IB'')$ 与 $\text{abs}(IC' - IC'')$ 变化曲线。根据所设定的阈值 ($T = 1$) 表明如 (b) 所示的音频数据已经被恶意篡改, (d) 所示的音频数据未被恶意篡改。(f) 为根据 (c) 对篡改进行定位所得波形。对比 (c) 与 (f), 可知所得的定位波形是比较准确的。

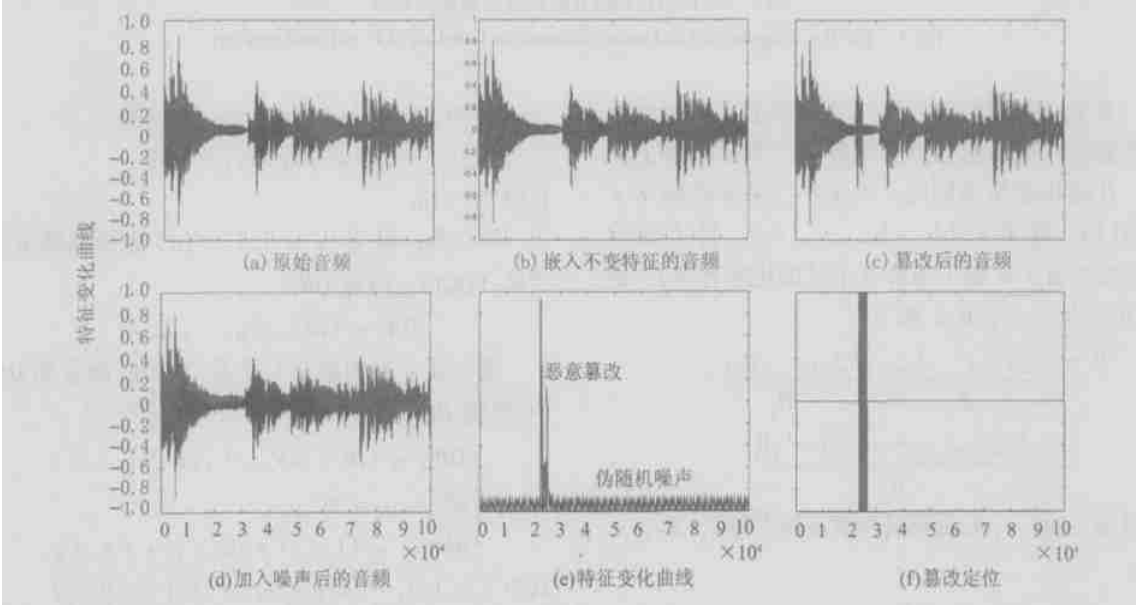


图 2 音频认证实验结果

Fig 2 The experimental results of audio authentication.

4 结 论

本文提出奇异值分解 (SVD) 与融合技术相结合的音频认证方法。原始音频奇异值分解后的奇异值作为不变特征嵌入利用融合嵌入到原始音频中, 认证时提取出不变特征作为认证码。该认证方法在认证时无须原始音频文件, 也不会造成数据的冗余, 实现了盲认证。实验表明, 该方法对随机噪声有鲁棒性, 并能对恶意篡改进行篡改定位。因此, 该方法是可行的, 能对音频文件的可靠性和真实性可进行较有效的认证。

参考文献:

[1] LU C S, LIAO H Y M, CHEN L H. Multipurpose audio watermarking Proc. 15th International Conf. on Pattern Recognition[C]. Spain, 2000.

[2] REGUNATHAN R, NASIR M. Audio Content Authentication Based on Psycho-Acoustic Model[EB/OL]. <http://citeseer.ist.psu.edu/Radhakrishnan01audio.html>

[3] KLEMA V C. The singular value decomposition: Its computation and some applications [J]. IEEE Trans Automatic Control, 1980, 25: 164~176

[4] 侯启槟, 杨晓帆, 王海涛, 等. 奇异值分解与 PKI 结合的鲁棒图像认证方法[J]. 计算机科学, 2004, 31(3): 145-149.

[5] 陈建华. 基于融合的数字声音隐藏方法[J]. 福州大学学报(自然科学版), 2001, 29(4): 104-105.

Blind Audio Authentication Algorithm Based on SVD and Amalgamation

WANG Xiao, BAI Sen, ZHAO Bo

(Chongqing Communication Institute, Chongqing 400035, China)

Abstract: To verify the authenticity and integrity of audio, we present an audio authentication method, in which singular value decomposition (SVD) is used to extract singular value as invariable features of host audio. Combining with amalgamation, we insert these extracted features into the host audio at the sender. Then at the receiver, we extract inserted features as authentication code, and compare them with those features from SVD. After setting proper threshold, we can make our judgments at last. Experimental results show that the proposed method not only can distinguish Gaussian noise from malicious tampering but also can detect where tampered regions are.

Key words: audio authentication; singular value decomposition (SVD); amalgamation; watermarking

(上接第 187 页)

Model based Steganalysis

YU Xiao yi, TAN Tie niu, WANG Yun hong

(NLPR, Institute of Automation, CAS, Beijing 100080, China)

Abstract: To consider a new method for performing steganalysis using a statistical model of the cover medium. Using model based methodology, examples of detecting secret message and estimating the secret message length of bit streams embedded using JSteg-like steganography and quantization index modulation are proposed. This steganalysis technique is based on the model of statistical distribution of quantized DCT coefficients. The histogram of cover image and “shrinkage histogram” are estimated from stego image using the statistical model. Then the secret message is detected and the secret message length is estimated. The methodology described in this paper is a framework which can also be applied to virtually any type of media such as JPEG2000 file format embedding.

Key words: steganalysis; DCT; QIM