# 公钥鲁棒性水印方案中水印信号的研究*

胡延军, 马小平, 陈 颖, 高 莉
(中国矿业大学信电学院, 江苏 徐州 221008)

摘 要: 公钥鲁棒性水印方法无疑是更具有应用前景的鲁棒性水印方案。提出了一种新的具有特殊相关特性的信号的产生方法; 并以此信号为水印信号, 实现了一种具有公钥鲁棒性数字水印方案。仿真实验结果证明基于该水印信号的公钥鲁棒性水印方案是可行的。

关键词: 鲁棒性水印; 公钥; 自相关
中图分类号: TP309 文献标识码: A 文章编号: 0529-6579 (2004) S2-0200-05

作为对数字媒体的版权保护技术的数字水印(digital watermarking) 技术, 目前已成为图像研究领域中新的研究热点之一[1-4]。按不同的标准, 数字水印技术可以有不同的分类方法。其中, 按数字水印的稳健特性, 数字水印可分为[5]: 可用于判断数字媒体是否被篡改过的脆弱性水印 (fragile watermarking), 和能经受各种数字信号处理的鲁棒性水印 (robust marking)。

从另一个角度看, 我们可以将数字水印技术分为公钥数字水印技术和非公钥水印技术。公钥水印技术就应如密码学中的公钥加密技术一样, 应该是一种除了密钥不能公开外, 其他一切细节都是可以公开的水印算法。从水印技术的实用化来看, 公钥水印方案应该更具有应用前景。借助于传统的加密技术, 目前脆弱性水印已提出了相应的基于传统加密方案的公钥算法, 如文献 [6]。而鲁棒性版权水印算法目前还基本上没有相应的公钥算法。

本文就对公钥鲁棒性水印方案进行了探索, 提出了一种公钥鲁棒性数字水印方案, 并为该方案设计了一种具有特殊相关特性的随机序列。

## 1 公钥鲁棒性水印算法思想

公钥鲁棒性水印是将版权信息隐藏在相应的被保护对象中。因此, 公钥鲁棒性水印算法从工作目的和过程看, 可将其分为 3 个过程:

(1) 水印的嵌入: 这个过程的目的是将版权信息也就是水印信号嵌入到载体 (即相应的数字作品或数字媒体) 中。

此过程的基本工作步骤如下: 首先利用变换函数 TF( ·) 对要被保护的数字媒体 $C_0$ 进行变换, 得到相应的向量 $R_0 = \mathrm{TF}(C_0)$; 然后利用水印嵌入 Em( ·) 函数, 以及秘密陷门 α 将水印信号(也是密钥信号) $W$ 嵌入到 $R_0$ 中, 得到相应的向量 $R'_0 = \mathrm{Em}(R_0, W, \alpha)$; 用 $R'_0$ 取代 $R_0$, 并利用 TF( ·) 的逆函数, 得到相应的含水印的数字媒体 $C_W = \mathrm{EF}^{-1}(R'_0)$。在这个过程中, 还要利用单向 /伪单向函数 Cy( ·) 建立一个和水印信号相关的公钥信号 Pub $k$ = Cey ( $W$)。

(2) 水印信号存在与否的判断: 这个过程执行的目的是用来判断某个数字媒体是否被版权保护。该过程最终只需要提供 1 bit 的信息, 即: 某个数字作品中是否含有某一公开的版权信息。

此过程的基本工作步骤如下: 假设待检验的数字媒体为 $C_u$, 则对 $C_u$ 进行和水印嵌入过程中相同的变换, 可得相应的 $R_u = \mathrm{TF}(C_u)$; 利用 Pub $k$ 以及水印检测函数 Det( ·) 对 $R_u$ 进行检测, 得 1 *bit* 信息 Ans = Det( $Pk$, $R'_0$)。该比特信号就回答了 $C_u$ 是否是受数字水印的保护。

(3) 版权主张者身份的验证: 这个过程是用来鉴别版权所有者身份。与第 2 个过程相对比, 它解决的问题是: 某个声称是作品的版权所有人, 到底是否确实是拥有版权的所有者? 对版权主张者验证其是否是真正的版权所有者, 其判断依据是看版权主张者是否可以将版权信息“干净”的擦除掉。

此过程的基本工作步骤如下: 版权主张者先进行水印嵌入过程的逆过程, 然后再进行水印存在与否的验证过程。如果版权主张者确实是版权所有者, 则他 /她进行完水印嵌入的逆过程后, 水印检测器将检测不到相应的水印信号。

* 收稿日期: 2004-09-11
作者简介: 胡延军 (1974 年生), 男, 讲师; E-mail: yjhu@cumt.edu.cn

在上述的3个过程中，单向/为单向函数Cy(·)的存在保证了密钥信号成为公钥，同时保证了不能从公钥中提取除密钥。而密码限门的存在则保证了不能利用水印嵌入算法的公开性中抹去密钥。同时，水印存在的判断检测和水印的嵌入算法是2个不对称的算法，进一步保证了算法的抗攻击性。

特别需要指出的是，算法中除了密钥和秘密限门不能公开外，算法的其他细节都可以公开。因此一般的信号无法作为水印信号，本文就设计了一种具有特殊相关特性的信号作为水印信号。

## 2　水印信号

### 2.1　最佳正弦伪随机序列

文献[7]提出：如果$b$是$p$的原根，则$1/p$为$b$进制全循环小数，由该全循环小数可产生最佳正弦伪随机序列$X=\{x_i\}$。可得$\tau=0\sim p-2$时周期自相关函数为：

$$R_{X,X}(\tau)=\frac{1}{p-1}\sum_{i=1}^{p-1}x_ix_{i+\tau}=\begin{cases}\dfrac{p}{2(p-1)} & \tau=0\\ -\dfrac{p}{2(p-1)} & \tau=\dfrac{p-1}{2}\\ 0 & 0<\tau<p-1,\ \tau\neq\dfrac{p-1}{2}\end{cases}\tag{1}$$

文献同时还证明了该序列是一种具有最多数的具有非常好随机特性的序列。

### 2.2　扩展最佳正弦伪随机序列

无疑最佳正弦伪随机序列具有很好的独特的相关特性，并且其抗干扰能力也比较强，但不能用它作为公钥鲁棒性数字水印中的密钥，因为序列的长度就泄漏了密钥信息。本文在该序列的基础上，设计了一种新的具有较好相关特性并可用作公钥鲁棒性水印密钥的随机序列的产生方法。

**2.2.1　密钥序列的产生方法**　在最佳正弦伪随机序列中的第$k$个数前插入数$I$，其中$1\leqslant k\leqslant p$，$I=p$。称扩展最佳正弦伪随机序列(EOPSS)，并记成EOPSS$(I,k,p,b)$。

**2.2.2　序列的自相关性质**　对序列$Y=\{y_i\}$作$p$的周期延拓，当$p$较大时，$\tau=0\sim p-1$序列自相关函数为[1]：

$$R_{Y,Y}(\tau)=\frac{1}{p}\sum_{i=1}^{p}y_iy_{i+\tau}\approx\begin{cases}0.5 & \tau=0\\ -0.25 & \tau=\dfrac{p}{2},\dfrac{p}{2}+1\\ 0 & 0<\tau<p-1;\ \tau\neq\dfrac{p}{2},\dfrac{p}{2}+1\end{cases}\tag{2}$$

从式2可以看出，利用本算法产生的序列具有非常独特的相关性质。对某个EOPSS$(I,k,p,b)$，其自相关函数和参数$I$、$k$几乎无关。对2个$p$、$b$相同而$I$、$k$不同的EOPSS序列，其自相关函数非常相似。因此，在公式(2)的基础上，公钥鲁棒性水印算法可具体如下设计。

## 3　公钥鲁棒性水印算法的实现

先定义2个函数：

(1) 2个序列长度都为$p$的序列$X=\{x_i\}$和$Y=\{y_i\}$，$i=0\sim p-1$。定义其相关函数为：

$$R_{X,Y}(\tau)=\frac{1}{p}\sum_{i=0}^{p-1}x_iy_{i+\tau}\tag{3}$$

其中，$i+\tau$作$i+\tau(\mathrm{mod}\ p)$理解。

(2) 2个序列长度都为$p$的序列$X=\{x_i\}$和$Y=\{y_i\}$，$i=0\sim p-1$。定义其区别度函数为：

$$\mathrm{Diff}(X,Y)=\sum_{i=0}^{p-1}\left|\frac{x_i}{2\lceil x_1\rceil}-\frac{y_i}{2\lceil y_1\rceil}\right|\tag{4}$$

### 3.1　水印信号的生成

水印信号是若干个扩展最佳正弦伪随机序列按下式构成：

$$W=\sum_{j=0}^{m}\mathrm{EOPSS}(I,k_j,p,b)\tag{5}$$

对水印信号，根据公式(2)以及经验，可以得到：当$\{k_j\}$中的各个元素之间的距离大于$p/10$时，有

$$R_{WW}(\tau)\approx\begin{cases}0.5\ \mathrm{m} & \tau=0\\ -0.25\ \mathrm{m} & \tau=\dfrac{p}{2},\dfrac{p}{2}+1\\ 0 & 0<\tau<p-1;\ \tau\neq\dfrac{p}{2},\dfrac{p}{2}+1\end{cases}\tag{6}$$

### 3.2　公钥的生成

公钥是由私有密钥通过某伪单向函数生成的。在本算法中，公钥可利用下式产生。即：

$$\mathrm{Pub}\ k=W+\mathrm{Rnd}(p)\tag{7}$$

其中，$\mathrm{Rnd}(p)$表示长度为$p$的随机信号。

由于作为水印信号的$W$序列本身具有较好的随机特性，因此，可以认为只知道Pub $k$是无法分解出相应的$W$。特别需要提出的是，在生成公钥前后，是不需要知道式(7)中的$\mathrm{Rnd}(p)$具体是什么值。

### 3.3　水印嵌入过程

(1) 根据式(5)产生相应的水印信号$W=\{w_i\}$，其中产生水印信号的各个参数作为密钥；同时根据式(7)，生成相应的公钥Pub $k=\{\mathrm{Pub}\ k_i\}$。

（2）从原始数字媒体中按照规则 $\xi$ 抽取某个长度为 $p$ 的序列 $V$。规则 $\xi$ 如何选取，并没有什么具体的规定，但规则必须保证提取出的序列是原始数字媒体中不可缺少的部分。也就是规则 $\xi$ 保证了攻击者不能以丢弃提取出来的序列 $V$ 的方法来擦去水印信号。

（3）根据式：

$$V' = V + \alpha g\mathrm{Pri}\ k \tag{8}$$

得到新序列 $V'$。参数 $\alpha$ 作为秘密限门。

（4）用 $V'$ 取代 $V$，按规则 $\xi$ 的逆过程，得到相应含有水印信号 $W$ 的数字媒体。

3.4 水印存在与否的验证过程

（1）从待检验数字媒体中按照规则 $\xi$ 抽取某个长度为 $p$ 的序列 $V'$。

（2）按式（3）求出公钥 Pub $k$ 的的自相关函数 $A_{\mathrm{Pub}\ k,\mathrm{Pub}\ k}(\tau)$，以及序列 $X^*$ 和公钥 Pub $k$ 的相关函数 $C_{X^*,\mathrm{Pub}\ k}(\tau)$。

（3）按式（4）计算 $A_{\mathrm{Pub}\ k,\mathrm{Pub}\ k}(\tau)$ 和 $C_{X^*,\mathrm{Pub}\ k}(\tau)$ 区别度 $\sigma$。是否存在水印信号，可根据 $\sigma$ 值来判断：

①假如待检验数字媒体中存在水印信号：

根据式（3），（5）和（7），以及 $V$、Pri $k$ 以及 Random（$p$）之间的互不相关性，可得到：

$$C_{X^*,\mathrm{Pub}\ k}(\tau) \approx \alpha C_{\mathrm{Pri}\ k,\mathrm{Pri}\ k}(\tau) \tag{9}$$

也就是区别度 $\sigma$ 将比较小。

②假如待检验数字媒体中不存在水印信号：推导类似，此时区别度 $\sigma$ 将比较小。

因此，最后以 $\sigma$ 判断水印信号是否存在：当 $\sigma$ 小于某一门限值 $d$ 时，就可以认为存在水印；否则认为水印不存在。

3.5 版权所有证明过程

（1）由版权主张者提供校验密钥序列 VER＝$\{\mathrm{Ver}_i\}$ 和秘密限门 $\alpha'$。

（2）对数字媒体进行水印嵌入过程的逆过程操作，可以得到抽取后的数字媒体 $M'$。

（3）对抽取后的数字媒体 $M'$ 水印信号检测。当区别度 $\sigma$ 值在公开的置信区间 $\sigma \pm \mu$ 内，说明水印抽取成功，证明抽取者对该图像拥有版权；否则说明主张者不拥有图像版权。

用上述过程进行版权所有的证明是合适的。这是因为，如果版权主张者确实是版权所有者，也就是提供的密钥序列和秘密限门就是嵌入水印的密钥和秘密限门；则水印嵌入过程一切都可逆，也就意味着版权所有者可以将数字媒体中的水印信号清除掉，清除掉水印信号的数字媒体再进行一次水印信号检测，其结果必然是不存在水印信号。

## 4 试验结果

对水印算法进行了实验仿真，仿真是在 Matlab 6.1 平台上进行的。取要保护的数字媒体为 256×256 大小的灰度 Peppers 图像。各个参数取值情况：$p$＝313，$b$＝10，$\alpha$＝0.15；门限值 $d$ 取 50；$\xi$ 规则为取图像小波分解后逼进子图中系数大于 5.8 的前 $p$ 个小波系数的小数部分。

置信区间计算后选取 201.0345±10。

4.1 添加水印对视觉效果的影响

试验结果如图 1 所示。加水印信号后的图像和原始图像从视觉上看，没有什么区别，水印具有良好的不可感知性。试验结果为：含水印信号的图像和原始图像的 PSNR 值为 45.9622，区别度 13.7618。

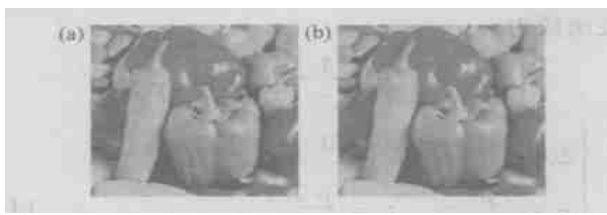


图 1 原始图像（a）和添加水印后（b）的图像

Fig. 1 Original image (a) and image watermarked (b)

4.2 常见图像处理对水印提取的影响

试验结果见图 2。其中：图 2a 是对含水印信号的图像加均值为 0，最大值为 0.1 的随机噪声；图 2b 是对含水印信号的图像加均值为 0，方差为 0.02 的高斯噪声；图 2c 是对含水印信号的图像模糊化，以仿真图像的打印后再扫描；图 2d 是对含水印信号的图像进行中值滤波；图 2e 是对含水印信号的图像进行魏纳滤波；图 2f 是对含水印信号的图像进行随机剪切。


图 2 对水印信号进行常见处理图像结果

Fig. 2 The image results of experiment of common signal distortions to watermarked images

试验结果如表 1。

表 1　对水印信号进行常见的信号处理的试验结果

Tab. 1　Results of experiment of common signal distortions to watermarked images

| 项目 | 图 2a | 图 2b | 图 2c | 图 2d | 图 2e | 图 2f |
|---|---|---|---|---|---|---|
| PSNR 值 | 21.9778 | 16.1498 | 20.5796 | 27.7203 | 34.0737 | 16.0226 |
| 区别度 | 14.5253 | 15.5523 | 88.9695 | 23.7628 | 17.8228 | 26.2281 |

尽管水印对图 2c 提取的效果不佳，但此时，图像的视觉效果已经非常差。因此仍然可以认为算法对各种干扰和各种常见的图像处理都有较强的鲁棒性。特别是对图 2f 剪切部分重要信号的情况下，提取的水印信号仍然可信。

### 4.3　JPEG 压缩对水印提取的影响

由于算法是工作在小波域中，因此算法将具有较强的抗 JPEG 压缩能力。试验结果如下表 2 所示，从表中可以看出该算法确实具有较强的抗 JPEG 压缩攻击。

表 2　JPEG 压缩对水印判断的影响

Tab. 2　The effect of JPEG compression on watermark detection

| 品质因子 | 10 | 20 | 30 | 40 |
|---|---|---|---|---|
| PSNR 值 | 29.5070 | 31.9268 | 33.0070 | 33.6259 |
| 区别度 | 14.9338 | 13.8777 | 13.9589 | 13.7642 |
| 品质因子 | 50 | 60 | 70 | |
| PSNR 值 | 32.5169 | 33.8202 | 35.2183 | |
| 区别度 | 13.7804 | 14.0565 | 13.9372 | |

### 4.4　攻击试验

由于算法的公开性，攻击者可以非常清楚的认识到，算法能否被击破，完全取决于是否可以得到相应的水印信号。产生水印信号的众多参数中；$p$ 值可以根据公开水印长度得到。除此之外，攻击者将无法得到其他秘钥。

在实际创建水印信号时，应避免出现 $m=1$ 的情况。当 $m=1$ 时，水印信号就是 EOPSS 信号，从水印的性质可以看出，占主导地位的参数为插入的位置 $k$，获得 $k$ 就等于获得了水印信号全部。攻击者可以通过创建 $p$ 个不同密钥和公钥求自相关，和公钥相关性最大的信号就是水印信号。

## 5　结　论

试验证明，基于本文提出的基于具有特殊相关特性的伪随机序列，用于版权保护的公钥鲁棒性水印算法是可行的。并可以看出算法抗一般的图像处理攻击。本算法的时间复杂度取决于密钥的长度和水印的嵌入强度的可选空间。因此增加序列的长度、采用多个序列、或嵌入水印时采用多个嵌入强度，可以延长算法的穷举攻击时间，使破解变得更加不可能。在以牺牲抗干扰能力为代价的情况下，密钥产生参数 $I$ 可作为一个新的秘密限门，进一步扩大密钥空间，提高算法的抗穷举攻击能力。

算法成立依赖于提出的信号的特殊性质，即信号的自相关函数隐藏了信号的一些特性，但同时自相关函数又有着自己独特的选择性。同时，算法的抗干扰能力又依赖于信号自身的抗干扰能力。

本算法需要保存的密钥非常小，但公钥太长。公钥和嵌入水印具有相同的长度。同时，公式 (5) 是否是可被认为是伪单向函数，也是算法是否成立的基础。因此，是否存在除了穷举法之外潜在的攻击方法将直接决定算法的是否可实用化。

参考文献：


[1] PETITCOLAS F A P, ANDERSON R J, KUHU M G. Information hiding —— A survey[J]. Proc of the IEEE Special Issue on Protection of Multimedia Content, 1999, 87(7): 1062－1078.

[2] 杨义先, 钮心忻. 多媒体信息伪装综述[J]. 通信学报, 2002, 23(5): 32－38.

[3] 章毓晋. 中国图像工程: 2003[J]. 中国图像图形学报, 2004, 9(A)(5): 513－531.

[4] 刘振华, 尹萍. 信息隐藏技术及其应用[M]. 北京: 科学出版社, 2002.

[5] 宋玉杰, 谭铁牛. 基于脆弱性数字水印的图像完整性验证研究[J]. 中国图像图形学报, 2003, 8(A)(1): 1－7.

[6] WONG P W. A public key watermark for image verification and authentication // Proc of the IEEE International Conference on Image Processing(ICIP'98)[C]. Chicago, Illinois, 1998, 1: 455－459.

[7] 胡德文. 非线性与多变量系统相关辨识[M]. 湖南: 国防科技大学出版社, 2001: 54－59.


(下转第 208 页)

# Adaptive Audio Digital Watermark Algorithm Based on Psychoacoustic Auditory Model

*LI Yun jian*, *CHEN Liang*, *ZHANG Xiong wei*
(Institute of communications engineering, PLA University of Sciences and Technology, Nanjing 210007, China)

**Abstract**: A digital watermark algorithm based on psychoacoustic model is presented. Watermark is embedded in frequency domain. The audio signal is divided into segments first, then each segment is performed discrete fourier transform (DFT). The masking thresholds of all segments are estimated by psychoacoustic analysis. And the watermark is embedded into the low frequency subbands and below the masking thresholds adaptively. The acoustic impact is little and the audio signal embedded watermark is perceptually similar to the original. The simulated results demonstrate that the algorithm is reliable and robust.

**Key words**: digital watermark; masking effect; psychoacoustic model

---

(上接第 203 页)

# Research on Watermark Signal of Public-key Digital Watermarking Scheme

*HU Yan Jun*, *MA Xiao ping*, *CHEN Ying*, *GAO Li*
(School of Communication & Electronic Engineering,
China University of Mining and Technology, Xuzhou 221008, Jiangsu, China)

**Abstract**: A public-key robust watermarking scheme has more potential value of application. A signal with with special auto-correlation characteristic is proposed. Also a public-key robust watermarking scheme based on this signal is designed and experimented. The experiment result shows the scheme is valid and robust to common signal distortions and malicious attacks.

**Key words**: robust watermarking; public-key; auto-correlation