维普资讯 http://www.cqvip.com

基于扩频的非对称数字水印*)

Asymmetric Watermark Based on Spread Spectrum

邹潇湘　李锦涛

(中科院计算所数字化室　北京100080)

Abstract Watermark technology has been developed to tackle the problem of unauthorized copying and distribution of digital data. Many different schemes have been proposed in the last few years, but most of them are symmetric, i.e., the key used for watermarking embedding is just the same used for watermarking detection. However, in many applications we need an asymmetric scheme, where a private key is used for watermark embedding, and a public key is used for watermark detection. Recently some asymmetric watermark schemes have been proposed. In this paper, we study one watermark scheme based on spread spectrum. We propose a way to generate public/private key to prevent the cheat of the copyright owner, and reducing the information need for watermark detection. Then we study the some problems of the watermark detection, and give a modified watermark detection schemes.

Keywords Digital watermark, Asymmetric watermark, Spread spectrum, Random number

1. 引言

随着多媒体技术和网络技术的飞速发展和广泛应用，数字图像、音频和视频等多媒体数字产品愈来愈需要一种有效的版权保护方法，数字水印技术就是针对这一问题而提出来的。所谓数字水印技术，就是将数字、序列号、文字、图像标志等版权信息嵌入到多媒体数据中，以起到版权保护、秘密通信、数据文件的真伪鉴别和产品标志等作用[1]。

现有的数字水印算法，其中大多数在某种程度上都利用了扩频通信的思想。所谓扩频通信，是通过将频率扩展，在一个宽带信道中传送一个窄带信号。而数字水印技术的研究目的，是在宿主信号中传送水印信息，宿主信号如图像，音频和视频，可以视作宽带的信道，而水印信号如版权者的身份标识，可以视作窄带的信号。因此，数字水印技术利用扩频通信的思想是很自然的了。

传统的数字水印技术，大多是对称的，即用于水印检测的密钥，与用于水印的嵌入的密钥相同。对称水印存在以下缺点：在进行水印检测的时候，需要出示私人密钥。而私钥一旦暴露，攻击者就能够移去水印，从而背离了版权保护的目的，同时，还有可能带来水印伪造等问题。因此，近年来一些学者开始研究非对称的水印技术。所谓非对称数字水印，顾名思义，就是用于水印嵌入的密钥，不同于用于水印检测的密钥。非对称水印技术的一个典型应用是版权认证：版权所有者使用私钥，在数字产品中嵌入一个标识自己身份的水印，用户在购买产品时，可以用公钥来验证其中是否存在水印，以保证购买的是正版的产品。同时，由于用户不知道私钥，他也就不能移去或伪造水印。

2. 扩频非对称水印

扩频水印的基本思想是在宿主信号中添加一个随机噪声序列，通过相关运算来进行检测，如 Cox[2]和 Hartung[3]等人提出的方法，另外一些水印方案，虽然没有明确指出是采用了扩频技术，但也是建立在其基本思想之上的，如 Pitas[4]等人提出的方法。在 Cox[2]的方案中，水印检测需要用到原始的宿主信号，很显然，这种水印方案具有很大的局限性，因为水印检测时出示的原始宿主信号很容易暴露给恶意的攻击者，这正是这种方案的薄弱环节；另外，在一些情况下，要得到原始宿主信号代价极高，比如在网络上传输的视频中嵌入水印，在水印检测时就几乎无法得到原始的视频数据。

因此，一种较好的方案应该是在检测过程中不需要宿主信号，具有这种特征的水印称为盲水印。Hartung[3]等人就提出了一种基于扩频技术的、不需要原始宿主信号的视频数字水印算法，其基本思想如下。

我们用大写字母如 X 表示信号序列，小写字母带下标如 x_i 表示该序列中的第 i 个元素，$i\in Z^+$。

水印嵌入。

设 X 为宿主信号，如图像、音频、视频等，设 A：

$$a_i, a_i \in \{-1, 1\}$$

为待嵌入到宿主信号 X 中的信息比特序列。我们首先用一个大的因子 cr 将该离散信号进行扩展，得到序列

$$b_i = a_j, j\cdot cr \leqslant i \leqslant (j+1)\cdot cr$$

扩展后的序列 b_i 接着用一个放大因子 a 放大，再用一个二元随机序列 P：

$$P_i \in \{-1, 1\}$$

进行调制，得到水印信号 $w_i = a\cdot b_i \cdot p_i$。在宿主信号 X 上加上该水印信号，就得到嵌入水印的序列 S：

$$s_i = x_i + a\cdot b_i \cdot p_i$$

设信号 S 受到有意的或无意的攻击之后，变为信号 R。要检测 R 中的水印，只要将信号 R 与随机序列 P 相乘并且求和，由于 P 的随机性，以及 P 和 X 的统计无关性，我们有：

$$c_j = \sum_{i=j\cdot cr}^{(j+1)\cdot cr-1} p_i \cdot r_i \approx \sum_{i=j\cdot cr}^{(j+1)\cdot cr-1} p_i^2 \cdot a\cdot b_i = cr\cdot a\cdot b_i = cr\cdot a\cdot a_j$$

这样，就可以恢复所嵌入的信息：

$$a_j = sign(c_j) = \begin{cases} +1 & c_j \geqslant 0 \\ -1 & c_j < 0 \end{cases}$$

*)本文的研究工作得到中科院计算所创新课题"高性能媒体服务器"的资助。邹潇湘　博士生，主要研究领域为数字水印和 MPEG 编解码。李锦涛　教授，博导，主要研究领域为数字化技术。

维普资讯 http://www.cqvip.com

在这个方案中，随机序列 P 是水印嵌入和检测的密钥。如果知道了该随机序列，则很容易移去水印，因此该方案是对称的。Hartung[5]改进了该方法，实现了一个非对称的水印方案，其基本思想是将随机序列 P 的一部分公开。构造一个随机序列 P^p，该序列约 $1/n$ 的元素取自随机序列 P，其它元素则取随机值，即

$$p_i^p=\begin{cases}p_i & 1/n\text{可能性}\\ \text{随机取值}\{-1,+1\} & \text{其它}\end{cases}$$

将信号 R 与该随机序列 P^p 相乘求和：

$$c_j^p=\sum_{i=j\cdot cr}^{(j+1)\cdot cr-1}p_i^p\cdot r_i=\sum_{i=j\cdot cr}^{(j+1)\cdot cr-1}p_i^p\cdot p_i\cdot a\cdot b_i\approx\frac{1}{n}\cdot cr\cdot a\cdot b_i=\frac{1}{n}cr\cdot a\cdot a_j$$

同样也可以恢复所嵌入的信息：

$$a_j^p=sign(c_j^p)$$

随机序列 P^p 可以用来检测水印是否存在，同时，该序列不会完全暴露水印的嵌入位置，从而保证了用户无法从 P^p 获知水印是如何嵌入的，该方案是非对称的。

3. 水印算法分析与改进

上面所述的水印算法是一种既可用于对称情况，又可用于非对称情况的算法。由于利用了扩频的思想，实现比较简单，是一种盲水印方案。而由于序列 P 的随机性质，以及随机序列 P 和宿主信号 X 的统计独立性，水印的鲁棒性、视觉不可感知性、统计不可见性比较好。本文针对该算法中的一些重要环节和主要问题进行分析和适当改进，以求进一步完善数字水印的嵌入和检测技术，从而实现一个可实用的非对称水印系统。

3.1 水印检测所需信息量问题

我们来讨论非对称的情况。在水印检测时，需要用到随机序列 P^p，它就是水印检测时的公钥，该序列是由用户的私钥 P 生成的。用户要得到该序列，就必须完整地获得该序列，而为了检测一比特的水印信息，所需的随机序列 P^p 的长度为 cr，一般来说，为了保证可靠检测，扩展因子 cr 一般取值较大，比如说1000。也就是说，为了验证得到一比特的信息，必须传输一个长度为 cr 的随机序列 P^p，如果水印有 n 比特，则要传输长为 $n\cdot cr$ 的序列，这显然是不合理的。

一个显而易见的改进方法就是改变公钥的生成策略，原有的方案是从 P 生成 P^p，我们将这个过程反过来，先用一个随机数生成器的种子 s 生成 P^p，然后从 P^p 生成 P：

$$p_i=\begin{cases}p_i^p & 1/n\text{可能性}\\ rand\{-1,+1\} & \text{其它}\end{cases}$$

而由 P^p 生成 P，可以用一个密钥 k 来控制。

在这个方案中，k 是私钥，由 k 以及 s 来生成随机序列 P，并用 P 来嵌入水印。s 是公钥，由它作为随机数生成器的种子，来生成随机序列 P^p，来进行水印检测。水印只需要一个随机数的种子，同时，由于 P 不但与 P^p 相关，还与私钥 k 相关，也就保证了所嵌入水印的安全性。

3.2 水印嵌入者的欺骗问题

在改进的方案中，水印检测时用到的序列 P^p 是由一个随机数生成器得到的，这也从某种程度上避免了原有方案中所存在的水印嵌入者欺骗问题：用户接受到的信号 R 中根本不存在任何水印，但是，水印嵌入者声称其中存在水印，因为在原有的方案中，水印嵌入者可以这样构造序列 P^p：

序列 P^p 中约 $a/(n\cdot\bar{x})$ 的元素取值为 a_j，其它的值则随机选取，且保证随机选取的 $+1$ 和 -1 的数目是相等的，其中 $\bar{x}$ 为宿主信号的统计平均值。

用户在检测水印时

$$C_j^p=\sum_{i=j\cdot cr}^{(j+1)\cdot cr-1}p_i^p\cdot r_i\approx a/(n\cdot\bar{x})\cdot cr\cdot\bar{x}\cdot a_j=\frac{1}{n}\cdot cr\cdot a\cdot a_j$$

这样，用户就可以检测到由水印嵌入者所声称的水印，而实际上并没有嵌入这样的水印！

注意序列 P^p 的构造，值 $a/\bar{x}$ 是放大因子与宿主信号的统计平均值的比值，为保证水印的不可感知性，即嵌入的水印要求对宿主信号的影响尽可能低，该比值应该比较小，比如说小于1/10，同时 n 一般来说可以大于10，这样 $a/(n\cdot\bar{x})$ 的取值小于1/100，即序列 P^p 中 $+1$ 和 -1 的数目相差1/100，只要水印嵌入者精心构造，该序列仍可以满足一定的随机性质，因此，用户无法判断水印嵌入者是否进行了欺骗。

另外，也可以这样构造伪随机序列 P^p：如果想让用户检测到 $+1$，则选取序列中 $+1$ 所对应的位置的宿主信号的平均值比 -1 所对应的位置的宿主信号的平均值大（$\frac{1}{n}\cdot cr\cdot a\cdot a_j$），或者反之。由于知道宿主信号，这样的“随机序列”是很容易构造出来的。同样，用户也可以检测到实际不存在的水印。

即使 P^p 是由随机数生成器的种子 s 得到的，也必须防止水印嵌入者采用穷举法，来找到一个 s，通过 s 生成的序列 P^p 可以检测到一个实际上不存在的水印。

结合上面两点讨论，我们得到改进的私钥/公钥生成策略。

水印嵌入 设 k 为水印嵌入者的密钥，假设需要得到 n 个公钥。依次计算散列值 $g_1=H(k)$，$g_2=H(g_1)$，$g_3=H(g_2)$，…，$g_n=H(g_{n-1})$，然后将这 n 个数作为随机数生成器的种子，生成随机序列 P_1^p，P_2^p，P_3^p，…，P_n^p，通过这些序列来构造随机序列 P：序列 P 约 $1/n$ 的元素取自随机序列 P_1^p，约 $1/n$ 的元素取自随机序列 P_2^p，约 $1/n$ 的元素取自随机序列 P_3^p，…，约 $1/n$ 的元素取自随机序列 P_n^p。从序列 P_1^p，P_2^p，P_3^p，…，P_n^p 构造序列 P 的过程由密钥 k 来控制。

让我们来考虑某个 $P_i^p(1\leqslant i\leqslant n)$ 与随机序列 P 的关系，P 的约 $1/n$ 的元素取自 P_i^p，而其余的元素取自其它的 $P_j^p(1\leqslant j\leqslant n, j\neq i)$，由于序列 P_1^p，P_2^p，P_3^p，…，P_n^p 两两之间是统计独立的（当然，这一点需要好的散列函数 H 和随机数生成器来保证），因此 P_i^p 和 P 之间满足这样的关系：P_i^p 约 $1/n$ 的元素取自随机序列 P，其它的元素则取随机值，因此，P_i^p 就是我们所需要的公钥。

最后，水印嵌入者用随机序列 P 来嵌入水印。

水印检测 水印嵌入者可以先公开 g_n，用户可以根据 g_n 生成的随机序列 P_n^p 来检测水印，如果 P_n^p 受到了攻击，而使得用 P_n^p 无法检测出水印，则水印嵌入者可以公开 g_{n-1}，用户此时可以根据 g_{n-1} 生成的随机序列 P_{n-1}^p 来检测水印，同时，用户还可以验证 $g_n=H(g_{n-1})$，保证水印嵌入者没有进行欺骗。

即使暴露了所有的随机数的种子，由于随机序列 P 还与密钥 k 相关，因此用户也不能够重建随机序列 P。当然，如果公开了过多的公钥，用户可以不必推导 P 而直接移去部分水印信息，这是由于这种扩频水印方案的本身特点所决定的[6]。

3.3 水印检测算法的改进

水印检测采用上述的相关运算，为了达到较好的检测效果，要求采用一个很大的扩展因子 cr。这是因为，采用一些常用的随机数生成算法，如 LFSR、A5等，并不能完全保证所生

维普资讯 http://www.cqvip.com

成序列中+1和-1的数目完全相等，设这些序列中+1比-1的数目多 m（小于0表示前者比后者少），这样，在水印检测时

$$c_j=\sum_{i=j\cdot cr}^{(j+1)\cdot cr-1}P_i\cdot r_i\approx m\cdot\bar{x}+(cr-|m|)\cdot a\cdot a_j$$

我们不妨设 $\bar{x}$ 和 a 非负，因此，m 对水印检测的影响如下：

表1 m 对水印检测的影响

a_j	m	c_j 的预期值	m 对的 c_j 影响
+1	>0	>0	增大
+1	<0	>0	减小
-1	>0	<0	增大
-1	<0	<0	减小

可以看出，其中第1和第4种情况使得 c_j 的绝对值增加，这对水印检测是有利的，但是，第2和第3种情况使得检测值 c_j 的绝对值减小，这使得检测的可靠性降低了。考虑最差的情况，水印检测的可靠性降低了。当然，这种影响还与宿主信号的平均值 $\bar{x}$ 有关，比如在小波变换域的低频系数中嵌入水印，小波低频系数的平均值是远大于0的，这时的影响就较大；而如果是在中频系数中嵌入水印，小波中频系数的平均值为0，这时的影响就相对较小，然而，为了保证水印的鲁棒性，我们常常需要将水印嵌入到低频系数中去。

第一种解决办法减少随机序列的偏差，使 m 的值趋向于0，这可以通过异或多个位，变换映射，压缩和快速傅立叶变换等方法来实现。

第二种方法是改变水印检测算法。原来的水印检测是通过计算 R 与 P 之间的相关性来实现的，我们这里改进了检测算法。

首先来考虑对称的情况，即水印检测时用到随机序列等于水印嵌入时的随机序列 P，分别计算：

$$v_j^+=\sum_{\substack{i=j\cdot cr\\ p_i=+1}}^{(j+1)\cdot cr-1}r_i\Big/\sum_{\substack{i=j\cdot cr\\ p_i=+1}}^{(j+1)\cdot cr-1}1\approx\bar{x}+a\cdot a_j$$

和

$$v_j^-=\sum_{\substack{i=j\cdot cr\\ p_i=-1}}^{(j+1)\cdot cr-1}r_i\Big/\sum_{\substack{i=j\cdot cr\\ p_i=-1}}^{(j+1)\cdot cr-1}1\approx\bar{x}-a\cdot a_j$$

其中 $\bar{x}$ 为宿主信号的统计平均值。

计算：

$$v_j=v_j^+-v_j^-\approx(\bar{x}+a\cdot a_j)-(\bar{x}-a\cdot a_j)=2a\cdot a_j$$

得到

$$a_j=sign(v_j)$$

本方法的基本思想是分别对随机序列 P 中+1和-1所对应位置的信号求统计平均值，因此，并不严格要求随机序列 P 中+1和-1的数目完全相同。

在非对称的情况下，即水印检测时用到的随机序列 P' 与水印嵌入时的随机序列 P 约有 $1/n$ 相同，而其余的部分随机选取，采用同样的检测方案，有：

$$v_j^+=\sum_{\substack{i=j\cdot cr\\ p_i'=+1}}^{(j+1)\cdot cr-1}r_i\Big/\sum_{\substack{i=j\cdot cr\\ p_i'=+1}}^{(j+1)\cdot cr-1}1\approx\frac{\frac{1}{2n}cr\cdot(\bar{x}+a\cdot a_j)+\frac{n-1}{2n}cr\cdot\bar{x}}{\frac{1}{2}cr}$$

$$=\bar{x}+\frac{1}{n}\cdot a\cdot a_j$$

和

$$v_j^-=\sum_{\substack{i=j\cdot cr\\ p_i'=-1}}^{(j+1)\cdot cr-1}r_i\Big/\sum_{\substack{i=j\cdot cr\\ p_i'=-1}}^{(j+1)\cdot cr-1}1\approx\frac{\frac{1}{2n}cr\cdot(\bar{x}-a\cdot a_j)+\frac{n-1}{2n}cr\cdot\bar{x}}{\frac{1}{2}cr}$$

$$=\bar{x}-\frac{1}{n}\cdot a\cdot a_j$$

计算：

$$v_j=v_j^+-v_j^-\approx\frac{2}{n}\cdot a\cdot a_j$$

得到

$$a_j=sign(v_j)$$

采用这种方法来检测水印，受随机序列的偏差影响较小，在 Pitas[4] 中也是采用类似的方法进行水印检测的，但是，其算法只是针对数字图像，而且没有提及扩频的思想，并且由于其检测采用了求数学期望、方差等方法，在处理上要复杂一些。

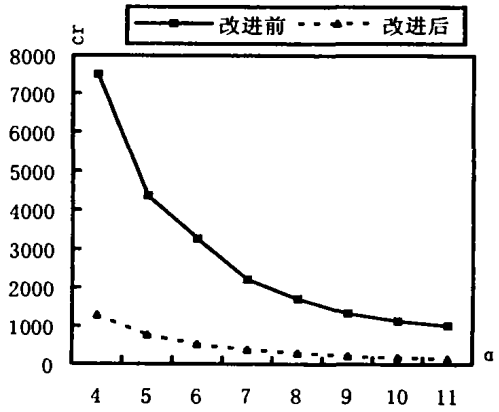

图1 对称检测

我们对一组(50幅)352×288的图像进行测试，在其 Y 分量(亮度)小波变换域的低频系数上进行水印的嵌入和提取。图1表示在给定的放大因子 α 下，为保证误差小于给定值，扩展因子 cr 应取的大小，实线部分代表原方案，误差取小于10%，虚线代表改进的方案，误差取小于3%。可以发现，即使误差要求提高了，改进的方案所需的扩展因子比原方案也大大减小，即对一段固定长度的宿主信号，改进的方法能够嵌入更多的信息量。

总结 扩频水印是目前广泛采用的一种水印技术。采用扩频水印技术，结合人类的视觉(听觉)的心理模型和掩蔽效应，能够实现较高的鲁棒性、不可感知性和安全性。本文对一种基于扩频的水印算法进行了研究，首先，提出了新的公钥/私钥的生成方法，能够有效地防止水印嵌入者的欺骗，且水印检测只需少量的信息。本文还对这种基于扩频的水印检测算法进行了研究，分析了其中可能存在的问题，并提出了一种新的水印检测方案。实验证明，新的方案在鲁棒性、水印嵌入量等方面都有较大的改进。

参考文献

1 高文，刘峰，黄铁军，等. 数字图书馆. 北京：清华大学出版社，2000

2 Cox I J ，et al. Secure Spread Spectrum Watermarking for Multimedia. IEEE Trans. on Image Processing，1997，6：1673～1687

3 Hartung F ，Girod B. Digital Watermarking of Raw and Compressed Video. In：Proc. SPIE 2952：Digital Compression Technologies and Systems for Video Communication，Oct. 1996. 205～213

4 Pitas I. A method for signature casting on digital images. Proc. of Intl. Conf. on Image Processing，1996(3)：215～218

5 Hartung F ，Girod B. Fast Public-Key Watermarking of Compressed Video，In：Proc. of the IEEE Intl. Conf. on Image Processing 1997 ，Santa Barbara，CA，USA，Oct. 1997

6 Eggers J J，et al. Asymmetric Watermarking Schemes，Sicherheit in Mediendaten，GMD Jahrestagung，Proceedings，Springer Verlag，2000