文章编号 1004-924X(2002)03-0247-06

基于小波变换的图像自适应盲水印算法

王 沛[1], 余松煜[1], 袁晓兵[2]
(1. 上海交通大学 图像通信与信息处理研究所, 上海 200030;
2. 中国科学院上海小 卫星工程部, 上海 200050)

摘要: 随着计算机和网络技术的飞速发展, 数字图像、音频和视频产品越来越需要一种有效的版权保护方法, 所谓数字水印就是一种嵌入到图像、视频或音频数据中的不可见标志, 可以用于多媒体数据的版权保护、认证和标注等。本文提出了一个有效的静止图像的自适应盲水印算法, 在水印检测过程中不需要原始图像。原始图像经小波变换后, 选择内嵌水印所需要的子带, 水印根据邻居特征平均值法和奇偶判决法内嵌到频域中所选择的子带上。实验结论和攻击测试表明, 本文所提议的算法具有较好的透明性, 对如 JPEG 有损压缩、中值滤波、附加噪声、伸缩、裁剪等各种图像处理的攻击有较强的顽健性。

关 键 词: 数字水印; 小波变换; 邻居特征平均值; 奇偶判决法
中图分类号: TP391 文献标识码: A

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, 通过网络获取、交换和传输图像、音频、视频等多媒体内容变得异常容易, 有恶意的个人和团体在没有得到多媒体数据文件所有者许可的情况下, 能肆意地复制和传播有版权保护的多媒体数据, 因此多媒体数据的保护成为迫切需要的问题[1]。而数字水印作为多媒体内容保护的新技术, 成为人们越来越重视的研究课题。数字水印技术是将与多媒体内容相关或不相关的一些标示信息直接嵌入多媒体内容当中, 但不影响原内容的价值, 并不能被人的知觉系统觉察或注意到。通过这些隐藏在多媒体内容中的信息, 可以达到确认内容创建者、购买者, 或者内容是否真实完整的目的。

针对不同的应用, 对水印的要求不同或者强调的重点不同, 对于静止图像中用于版权保护的水印一般应具有如下特性:

不可感知性 —水印技术的首要条件是加入水印的图像和原始图像基本上相同, 即水印是看不见的, 图像的质量不因水印的加入有明显的改变, 否则将影响图像的商业价值。

顽健性 —加入水印的图像在传播过程中必然会受到各种有意或无意的干扰, 如网上传播常用的有损压缩、经过信道可能附加的噪声、常用的一些图像处理技术, 如图像缩放、裁剪、灰阶调整等, 水印技术必须能抵抗住这些干扰和常见的信号处理。另外, 水印技术还应能抵御各种有意破坏和恶意篡改, 如去除水印和破坏水印, 使水印无法提取的行为。

隐藏能力 —是指在不影响图像质量的前提条件下, 能加入水印的信息量。为了加入足够的版权信息来作为合法证据, 水印算法应有合理的隐藏能力。

数字水印概念的提出仅有短短几年, 正处于发展初期阶段, 从理论上到实际应用都有许多问题有待于解决。这几年提出的数字水印方法通常可以分为两大类: 空间域数字水印方法和频率域数字水印方法。

空间域和频率域相比, 实施容易, 但顽健性差。Van Schyndel 等提出 LSB 法[2], 在空间域利用原图像数据的最低几位来隐藏数据, 水印提取是通过比较原始图像和加水印图像的每个最无意义位, 其算法简单, 但对压缩和图像处理不顽健。

收稿日期: 2001-09-21; 修订日期: 2002-04-18

Bander 等提出了 patchwork 方法[3], 这是一个基于统计的水印方法, 任意选择 n 对图像点(a_i, b_i), 增加 a_i 的亮度一个单位, 而降低 b_i 的亮度一个单位。此算法简单易行, 但对噪声不顽健。

在频率域内嵌水印需要更多的计算时间, 但可以嵌入大量数据而不会导致可察觉的缺陷, 并有对噪声和压缩顽健性的优点。频率域水印最常用的图像变换是离散余弦变换(DCT)和小波变换。Cox 等人提出了基于图像全局 DCT 的水印方法[4], 并受通讯中扩频的启发, 将窄带信号扩展为宽带信号来隐藏信息, 所有水印内嵌和提取步骤都在频率域进行, 此方法的问题是水印系数的不明确性导致检测水印信息的艰难和在 DCT 系数的低频区域内嵌水印所导致的几何失真。一般来说基于小波的水印方法在图像的视觉透明性和顽健性方面要好于基于 DCT 的水印方法, 其中最有代表性的是 Podichuk I 等提出的基于小波变换的水印方法[5], 利用视觉模型来判断水印加在图像上的位置及可加水印强度的上限。许多基于小波的水印算法都是在此基础上发展的, 将水印隐藏在子带的有意义大系数上, 即保证水印的不可见性, 又能尽可能地增大水印强度来抵抗压缩等攻击, 但由于受加水印位置的限制, 这类方法有最大的几个缺点: 所能隐藏的水印容量小; 对几何攻击脆弱; 不易实现盲水印。

迄今为止, 大部分提议的水印算法尤其是基于小波的水印算法在检测水印时, 都需要将加水印后的图像与原始图像进行比较以提取水印, 不能与水印在网络和数字图书馆上的自动验证结合起来, 所以水印的新热点是盲水印, 即不需要原始图像数据进行水印检测的水印算法。已经有一些研究者提出了一些盲水印算法, 但由于水印检测必须脱离原始图像数据局限了水印内嵌算法, 这些算法的顽健性受到了影响。

本文提出的一种新的图像自适应盲水印算法, 水印用提出的相邻特征平均值和奇偶判决法在图像的小波域上内嵌水印, 该方法自适应于图像特征, 并且在水印检测过程中算法简单、不需要原始图像。根据本算法的实验结果, 该算法具有水印隐藏效果好, 对不同攻击如 JPEG 有损压缩、附加噪声、图像缩放、裁剪、灰阶调整等各种图像处理顽健性好等优点。

2 主要研究内容

数字水印方法一般包括水印内嵌处理过程和水印提取过程。

2.1 水印内嵌处理

图 1 显示了本文整个水印内嵌处理的基本步骤, 其中加阴影的系数即表示内嵌水印的系数。原始图像经过小波变换后, 选择所需要的子带, 用相邻特征平均值算法, 根据所需要嵌入的水印值的不同, 在子带的系数上进行不同修改, 将来产生的随机水印信号嵌入到图像中。

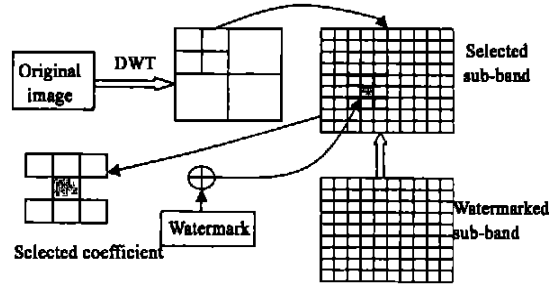


图 1　水印内嵌处理的基本步骤

Fig. 1　Watermark embedding procedure.

内嵌步骤:

1) 原始图像的小波分解和加水印子带的选择

小波变换是构建一个分级的子带系统, 它具有多分辨率特性和分级结构, 以及没有 DCT 的方块效应等优点。原始图像进行 L 阶离散小波变换后, 产生一个低频子带 LL 和相应于每级分解阶上的水平、垂直和斜向方向上的细节子带序列 $LH_i, HL_i, HH_i (i = 1, 2, \cdots\cdots L)$。

因为本文水印算法的特点是检测时需要利用小波系数之间的相关性, 而不同子带的系数之间相关性较小, 所以决定选择同一分解阶的同一个子带上的系数内嵌水印。LL 低频子带因为包含图像的重要信息不适合内嵌水印, 否则会带来图像的质量退化, 容易被人眼感知。在最低阶子带 LH_1, HL_1, HH_1 上内嵌水印虽然会带来知觉上的低可见性, 却不可避免地易受类似低通和中值滤波的攻击。而在例如 LH_3, HL_3, HH_3 等高阶子带上内嵌水印, 由于这些子带小, 所能内嵌的水印信号容量小, 同时水印信号也不能完全覆盖到整

幅图像上, 无法有效抵抗裁剪等攻击。HH_i 子带也有缺点, 因为此类子带在视觉上不敏感, 大多数有损压缩算法都针对这样一个不敏感区域, 导致内嵌水印的低生存率。由于将水印插入上述这些子带将降低顽健性(尤其对于压缩和低通滤波), 因此最后决定图像只进行 2 阶分解, 并决定水印内嵌位置为中阶区域的水平子带和垂直子带, 即 LH_2 子带和 HL_2 子带。

原始图像用离散小波变换(DWT) 作 2 阶分解, 选择 LH_2 子带和 HL_2 子带其中之一来内嵌水印, 具体选择方法如下:

分别计算 LH_2 子带和 HL_2 子带的方差 Var_{LH2} 和 Var_{HL2}, 所选择的子带 I 为其中具有较大方差的子带, 因为子带的方差越大, 表示其中的边缘纹理分量就越丰富, 适合隐藏信息, 不易被感知, 即

$$I = \begin{cases} LH_2 & Var_{LH_2} \geqslant Var_{HL_2} \\ HL_2 & Var_{LH_2} < Var_{HL_2}, \end{cases} \tag{1}$$

2) 水印的产生

通常所用的水印信号是伪随机序列信号, 因为不同长度的伪随机序列有无穷多个, 同一长度的伪随机序列也有许多个, 此外, 同一伪随机序列的起始相位也不相同, 序列周期越长, 解密需要探索起始相位所花费时间就越长, 所以作为水印的伪随机序列信号应具有较长的周期, 这增加了水印的安全性和保密性。

为了保证水印信号的唯一性, 在产生随机信号时, 一般将作者信息或设定的密钥作为随机信号的参数来使用, 即作为“种子”来产生一个伪随机序列信号, 这个伪随机序列信号就唯一取决于作者, 攻击者无法伪造水印信息。

以设定的密钥为“种子”产生伪随机序列 W, 设定其长度和所选择的图像小波分解后的子带相关, 为让这个任意数目适合所选择的 I 子带的尺寸, 伪随机序列长度 W_L 被设定为 I 子带上系数数目 S_I 的 $\frac{1}{4}$, 即

$$W_L = \frac{1}{4S_I}, \tag{2}$$

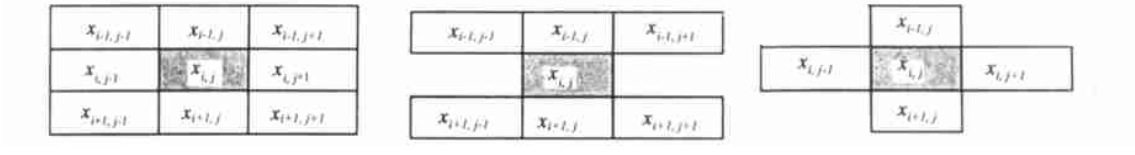
3) 邻居特征平均值的计算

计算选择系数的邻居特征平均值。首先将此子带上所有系数加上一个 f, 使所有系数都变成正数。f 为最大的 I 子带上系数绝对值, 具体公式如下:

$$f = \max_{x_{k,l} \in I}(|x_{k,l}|), \tag{3}$$

然后假如以 $x_{i,j}$ 表示此时子带上水印内嵌位置系数的值, 其相邻的邻居系数有 8 个, 分别是 $x_{i-1,j-1}$, $x_{i-1,j}$, $x_{i-1,j+1}$, $x_{i,j-1}$, $x_{i,j+1}$, $x_{i+1,j-1}$, $x_{i+1,j}$, $x_{i+1,j+1}$。对需要参加计算的邻居的选择可以有几种方案, ①选择 8 个邻居; ②选择 6 个邻居; ③选择 4 个邻居[6], 选择示意图如图 2 所示, 加阴影的系数表示是要内嵌水印的系数。经过加水印实验测试后的效果来看, 决定选择 6 个邻居参加邻居特征平均值计算。系数的邻居特征平均值是 $m_{i,j}$, $m_{i,j}$ 用如下公式计算:

$$m_{i,j} = mean(x_{i-1,j-1}, x_{i-1,j}, x_{i-1,j+1}, x_{i+1,j-1}, x_{i+1,j}, x_{i+1,j+1}), \tag{4}$$



(a) 8 邻居选择法　(b) 6 邻居选择法　(c) 4 邻居选择法

(a) 8 neighboring pixels　(b) 6 neighboring pixels　(c) 4 neighboring pixels

图 2　$x_{i,j}$ 像素的相邻邻居的选择

Fig. 2　Selection of $x_{i,j}$'s neighboring pixels.

因为此算法需要邻居的值, 为避免水印位置的交迭, 相当于在子带系数上隔行、隔点内嵌水印, 如图 1。而边界的处理是对边界系数进行对称循环扩展。

4) 奇偶判决法内嵌水印

在所选择的系数上内嵌水印的具体方法如下:

①首先将邻居特征平均值 $m_{i,j}$ 进行加权计算, 加权因子为 α, 修改后邻居特征平均值为 $m'_{i,j}$。

$$m'_{i,j} = \alpha m_{i,j}, \quad (5)$$

②计算标志 $k_{i,j}$。

$$k_{i,j} = round\left(\frac{x_{i,j}}{m'_{i,j}}\right), \quad (6)$$

$$x'_{i,j} = \begin{cases} k_{i,j}m_{i,j} & \bmod(k_{i,j},2) = 1 \\ (k_{i,j}-1)\cdot m_{i,j} & (\bmod(k_{i,j},2) = 0) \wedge (x_{i,j} \leqslant k_{i,j}, m_{i,j}) \\ (k_{i,j}+1)\cdot m_{i,j} & (\bmod(k_{i,j},2) = 0) \wedge (x_{i,j} > k_{i,j}, m_{i,j}), \end{cases} \quad (7)$$

当水印信号值为0时,即 $W = 0$ 时,

$$x'_{i,j} = \begin{cases} k_{i,j}m_{i,j} & \bmod(k_{i,j},2) = 0 \\ (k_{i,j}-1)\cdot m_{i,j} & (\bmod(k_{i,j},2) = 1) \wedge (x_{i,j} \leqslant k_{i,j}, m_{i,j}) \\ (k_{i,j}+1)\cdot m_{i,j} & (\bmod(k_{i,j},2) = 1) \wedge (x_{i,j} > k_{i,j}, m_{i,j}), \end{cases} \quad (8)$$

5) 再将此子带上所有系数减去 f,然后进行逆小波变换IDWT,产生加水印图像。产生水印随机序列信号的"种子"、加权因子 α 和选择加水印的子带 I 作为密钥,在水印检测时用到。

2.2 水印提取处理

水印检测是水印内嵌的逆步骤,在检测处理中,加水印图像首先进行小波变换,在已知所选择的子带上仍然用相邻特征平均值算法和奇偶判决法来提取水印,整个水印提取过程不需要原始图像数据。

提取步骤:

1) 加水印图像的分解

加水印图像进行2级DWT。

2) 产生原始水印

通过用水印检测步骤中相同的"种子"制造和在水印内嵌步骤中产生的相同的伪随机数目序列,即原始水印 W。仅有版权持有者才知道这把钥匙来确认版权。

3) 计算邻居特征平均值

在已知所选择的子带上,用水印内嵌步骤3所描述的步骤计算邻居特征平均值 $\hat{m}_{i,j}$。

4) 奇偶判决法提取水印

用水印内嵌步骤4所描述的步骤来产生 $\hat{m}'_{i,j}$ 和计算标志 $\hat{K}'_{i,j}$,然后依据以下公式来提取水印。

$$\hat{W} = \begin{cases} 1 & \bmod(\hat{k}'_{i,j},2) = 1 \\ 0 & \bmod(\hat{k}'_{i,j},2) = 0, \end{cases} \quad (9)$$

5) 最后用相似函数来测试原始水印数据 W 和提出的水印数据 $\hat{W}$ 之间的相似性,完成水印测试:

$$\mathrm{sim}(W,\hat{W}) = \frac{\sum_{n=1}^{W_L} W(n)\cdot\hat{W}(n)}{\sqrt{\sum_{n=1}^{W_L}\hat{W}^2(n)}}, \quad (10)$$

$\mathrm{sim}(W,\hat{W})$ 说明原始水印与提出水印的相似度,水印存在与否的判定标准为:若 $\mathrm{sim}(W,\hat{W}) > T$,就能判定被测试图像中有水印 W 存在,否则,没有水印。其中,T 为判断图像中是否有水印存在的阈值,T 的选择要考虑水印信号的错检率,即原始水印数据 W 和提出的水印数据 $\hat{W}$ 不相关时,$\mathrm{sim}(W,\hat{W}) > T$ 的概率。

3 实验数据和性能分析

我们使用LENA(512×512×8bits)图像作为测试图像,如图3,小波变换参数为Daubechies 9/7滤波器,小波分解为2阶。采用长度为4096的伪随机信号序列作为水印信号,由公式(10)可算出,此长度的水印信号检测相似度在提取的水印信号完全正确,无任何错误时,$\mathrm{sim}(W,\hat{W}) = 64$,而当 T 为6时,判断水印信号存在的错检率小于10^{-8},所以将 T 设定为6。公式(5)中加权因子 α 选择较大值能增强水印对图像处理的免疫力,但将导致一个相对于原始图像有较低逼真度的加水印图像,选择较小值能提高加水印图像的逼真度,但水印却容易被攻击破坏,通过对 α 的调节能有效折衷这对矛盾。一般来说,PSNR值在45dB以上可以保证加水印

图像的高保真性, 取 α = 0.08。加上水印后的图像如图 4, 内嵌水印后的图像 PSNR= 47.3064dB, PSNR 值和主观视觉效果都证实了应用所提议的方案实现的水印不可感知性。

图 3　原始图像

Fig. 3　Original image.

图 4　加水印图像

Fig. 4　Watermarked image.

将加水印图像针对容易遇到的攻击进行水印检测响应的相似度测试, 图 5 是 JPEG 有损压缩的攻击下的提取水印的检测响应曲线图, 其中 JPEG

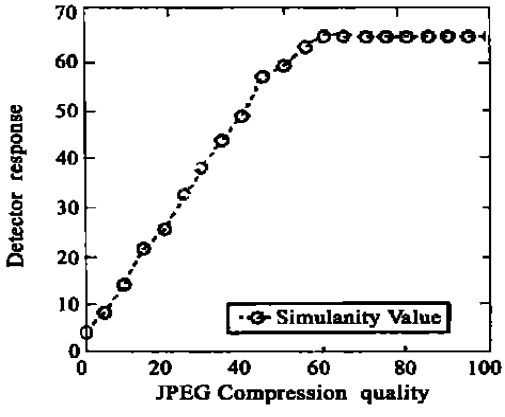


图 5　JPEG 有损压缩的检测响应曲线图

Fig. 5　Plot of the detector response corresponding to JPEG lossy compression quality.

压缩质量因子为 1 时, 压缩比大约为 27: 1。表 1 是加水印图像在几种常见的图像处理攻击下, 提取水印的检测响应测试数据, 攻击分别为中值滤波; 附加高斯噪声; 16 阶灰阶均衡器, 即将 256 阶灰度图像转换为 16 阶灰度图像; 图像尺寸缩小为 256 × 256; 图像尺寸放大为 1024 × 1024; 底片处理; 裁剪, 裁剪后的图像尺寸为 320 × 320, 如图 6 所示。

图 6　裁剪图像

Fig. 6　Cropped image (320 × 320).

由试验结果的图表可看出, 加水印图像的 PSNR 值很高, 水印隐藏效果好, 在所加水印强度不大的情况下, 面临如 JPEG 有损压缩、附加噪声、图像缩放、裁剪、灰阶调整等各种攻击, 图像的质量严重退化, PSNR 值下降的情况下, 即使 PSNR 值低到 10dB 左右, 水印仍然能很好地生存, 顽健性很好, 足以证明本文所提出的算法是一个有效的自适应盲水印算法。

表 **1**　在不同攻击下的提取水印的检测响应, 水印图像的 **PSNR** 值

Table 1　Detector responses of extracted watermarks, and PSNR values of watermarked image after various attacks

Attack types	Detector responses	PSNR values
No attack	64	47.3064
Median filter(5× 5)	11.69	32.0116
Gaussian noise (Variation 0.001, mean value 0)	17.7813	29.8522
16 gray level equalizer	25.0938	16.3742
Scale down to 256× 256	36.4688	29.3036
Scale up to 1024× 1024	63.5890	44.6578
Negative operation	53.8962	9.6464
Cropping	10.8283	

4　结论

本文讨论了一个有效的自适应盲水印算法, 原始图像经小波变换后, 水印用邻居特征平均值法和奇偶判决法内嵌到频域中。实验结论和攻击测试表明, 该算法具有较好的透明性, 对各种攻击及大多数图像处理技术有较强的顽健性, 尤其是基于小

波的水印技术所不易抵抗的裁剪等几何攻击,但此方法对于旋转还缺乏足够的顽健能力,今后将会作出进一步的改进。本文设计的水印算法自适应于图像特征,对各种攻击顽健性好,在水印检测过程中不需要原始图像,并且计算简单,尤其是检测过程的计算十分容易,适合网络和数字图书馆上的自动验证,是一个易于推向实用的水印算法。

参考文献:

[1] 杨洪波. 网上档案信息的安全及保密技术[J]. 光学 精密工程, 2000, 8(6): 591- 594.

[2] Osbone C F. A digital watermarking[A]. *Int. Conf. In: Image processing* [C]. 1994, 12: 86- 90.

[3] Bendor W. Techniques for data hiding[J]. *IBM System Tournal*, 1996, 38(4): 313- 336.

[4] Cox I J. Secure spread spectrum watermarking for multimedia[A]. *Image Processing, IEEE Transactions on* [C]. 1997. 1673 - 1687.

[5] Podilchuk C I, Zeng W. Image- adaptive watermarking using visual models[J]. *IEEE Journal on Special Areas in Communications*, 1998, 16(4): 525- 539.

[6] Ikpyo Hong. A blind watermarking technique using wavelet transform[A]. *Industrial Electronics*, 2001. *Proceedings. ISIE* 2001. *IEEE International Symposium on* [C]. 2001. 1946- 1950.

Adaptive blind watermarking algorithm based on wavelet transform

WANG Pei[1], YU Song_yu[1], YUAN Xiao_bing[2]

(1. *Institute of Image Communications and Information Processing, Shanghai Jiaotong University, Shanghai* 20030, *China;*
2. *Shanghai Micro_Satellite Department of Chinese Academy of Sciences, Shanghai* 20050, *Chian*)

Abstract: A digital watermark is an invisible mark embedded in digital images, video or audio documents, which may be used for a number of different purposes including copyright protection, authentication and captioning. In this paper, an effective adaptive watermarking algorithm for still images is porposed. This is a blind watermark confirming the copyright without the original image, which is transformed using wavelet transform, and the watermark is embedded in the selected subband of frequency domain according to neighboring symbol's mean value and odd_even adjugement rule. The experimental results and attack analysis show that the watermark algorithm is transparent and robust against some image processing operations, such as JPEG lossy compression, median filtering, additive noise, scaling, and incorporating attacks.

Key words: digital watermark; wavelet transform; neighboring symbol's mean value; odd_even adjudgement rule

作者简介:王 沛(1970-),女,四川省泸州市人,2000年博士毕业于中国科学院长春光机所,现为上海交通大学图像通信与信息处理研究所博士后,从事图像通信与信息处理工作。E_mail: wangpei@dushu.net。