

一种有意义的图像水印算法^{*}

王振武¹, 刘九芬^{2,3}, 黄达人³

(1. 中山大学计算机科学系, 广东 广州 510275

2. 中国科学院自动化所模式识别国家重点实验室, 北京 100080

3. 中山大学科学计算与计算机应用系, 广东 广州 510275)

摘 要: 提出了一个基于小波变换的有意义图像水印算法。该算法在 $512 \times 512 \times 8$ bits 图像上嵌入了一个 536 bits 的有意义字符串, 水印检测时不需要原始图像, 并借助于模板、登记图像的大小、纠错编码和二维交织技术, 水印不但可以对抗一般的信号处理, 还可以抵抗缩放、改变长宽比、伴随着剪裁的旋转和随机去行去列等几何攻击。

关键词: 几何攻击; 小波变换; 有意义水印; 二维交织; 模板

中图分类号: TP391 **文献标识码:** A **文章编号:** 0529-6579 (2003) 01-0001-04

稳健性是数字水印系统的一项基本要求。大量不同的水印算法广泛地提出了“稳健性”声明。不幸的是, 大多数水印算法所强调的稳健性只不过是水印对抗一般信号处理的稳健性能, 它们甚至不能抵抗微小的几何攻击。如果水印在提取过程中没有原始数据可供利用, 几何攻击的问题更加突出。

水印抗几何攻击的研究目前处于刚刚起步阶段。Pereira 等^[1-4] 利用在变换域嵌入模板 (Template) 来抵抗几何攻击。该类算法的模板由离散 Fourier 变换 (DFT) 幅度谱中额外的随机位置的极值点组成, 水印按不同的编码也嵌入到 DFT 域。水印检测时, 通过检查模板的变化, 决定水印图像可能遭受的几何攻击。对水印图像进行逆变换, 就可在 DFT 域内检测到水印。但上述算法的最大信息嵌入量是 100 bits, 而且算法集中于 DFT 域, 它们与新的图像压缩标准 JPEG 2000 不兼容因而限制了其应用。

由于 DWT (Discrete Wavelet Transform) 的良好性质, 使它成为 JPEG 2000 的核心技术, 并逐渐代替 DCT (Discrete Cosine Transform) 成为变换域数字水印算法的主要工具。但 DWT 同 DCT 一样, 不具有平移、旋转和缩放不变性, 使得它抗几何攻击的能力很差。因此, 如何解决 DWT 域水印抗几何攻击问题具有重要的意义。

本文提出了一个 DWT 域的盲检测的有意义图

像水印算法。该算法在以前工作的基础上^[5], 又利用了二维交织技术, 在 $512 \times 512 \times 8$ bits 的图像上嵌入了一个 536 bits 的字符串; 并借助于嵌入模板、登记图像的大小, 除了原有的可以对抗一般的信号处理外, 还可以抵抗 StirMark^[6] 的一些几何攻击。

1 有意义信息的嵌入

本文在以前利用 BCH 纠错编码工作的基础上^[5], 又利用了二维交织技术以提高水印的稳健性。某些攻击函数, 例如裁剪或者 jitter (随机去行去列), 会令其中嵌入的水印数据发生突发错误。对于功率受限的水印信息, 当一个码字中的错误比特数超过它的纠错能力时, 就会发生译码错误。而二维交织技术^[7] 试图使突发错误尽量分散到各个码字中, 降低一个码字中的错误比特数, 从而使原来不能纠正的突发错误得到纠正。

图 1 为图像水印嵌入框图。有意义水印 W 由长度为 L 的 ASCII 字符串构成。水印每个字节经过 BCH 编码, 然后按序连接起来可得到待嵌入主图像的二进制数据 X 。根据 X 数据量的多少, 尽量提高图像小波分解的级数, 对图像进行分解。这里把低频带 LL 系数先进行二维交织, 然后按行扫描变成一维数组, 并据文 [5] 把待嵌入主图像的二进制数据 X 嵌入到小波低频带系数中。对嵌入水印后的 LL, 先进行反交织过程, 再进行 BCH 解码

* 收稿日期: 2002-05-20

基金项目: 国家自然科学基金资助项目 (60133020, 60172067); 国家 863 计划资助项目 (2002AA144060); 广东省自然科学基金重点资助项目 (013164)

作者简介: 王振武 (1976 年生), 男, 博士; 通讯联系人: 刘九芬; E-mail: Liu.jiufen@163.net

和逆小波变换, 就得到了嵌入有意义信息的图像。一些具体细节可参见文 [5]。

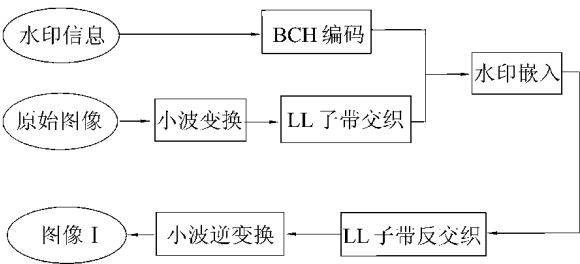


图 1 水印嵌入框图

Fig 1 Watemark embedding diagram

2 水印图像重同步

目前大多数水印算法不能抵抗几何攻击。原因在于, 对于给定的水印算法, 水印检测器必须知道嵌入水印的确切位置。包括仿射变换、裁剪以及 StirMark 攻击的几何变形趋向于破坏同步性, 使得水印嵌入和水印检测位置偏离不再相符。若水印算法没有明确设计抵御这种攻击, 则对这种攻击的补偿是十分困难的, 最主要的困难在于在载体数据中对原始水印参考点的寻找。本文通过嵌入模板、登记图像的大小, 抵抗一些几何攻击。

2.1 基于模板的重同步

本文也在 DFT 的幅度谱上嵌入模板。希望水印图像可能遭遇的旋转攻击能在模板上得以体现, 使我们有可能在提取嵌入的有意义信息之前, 通过反旋转, 使待检测图像和原始图像重同步, 从而取得最佳的检测效果。

由于 DFT 低频系数对模板干扰太大, 并且对图像旋转不够敏感, 小角度的旋转攻击, 嵌于低频带的模板不能很好地反映出来。而高频对常见图像的处理 (例如压缩) 不稳健。因此我们选择了 DFT 中频带来嵌入模板。图 2 为嵌入模板的示意图。

基于模板的算法描述

嵌入模板就是在水印图像 I 的 DFT 域的中频带中选择一定数量的点, 改变其幅度。方法如下:

- (1) 对嵌入有意义信息后的图像 I, 根据精度的要求, 图像 I 的四周适当补零得到一个大的图像, 计算 DFT 的幅度值, 得到相应的矩阵 M ;
- (2) 在幅度矩阵 M 的中频带区域 (离矩阵中心越近, 频带越低), 选择一定数量的点 (这儿选择了半径为 R 圆周上的点), 不妨设为 Num 个点;
- (3) 依次以这 Num 个点为中心, 选择合适大小的窗口, 不妨设为 $WinLen \times WinLen$, 并计算窗口内像素的局部平均值 A , 局部标准偏差 S ; 然后

用 $A + N \times S$ 值取代该点的原始值。

(4) 为了使改变后的幅度谱和原先得到的相位谱经过逆 Fourier 变换后得到的图像质量损失最小, 应该对称地改变幅度上的值 (见图 2)。这是因为 Fourier 变换具有共轭对称性, 幅度谱是关于图像中心一一对应的, 若不同时改变幅度谱中相对应的两点, 逆 Fourier 变换后会出现复值。相当于一次轻微的攻击。

注意: 图像在时域内旋转会引起 Fourier 变换域内旋转相同的角度, 所以半径为 R 圆周上的点也旋转相同的角度且仍在半径为 R 的圆周上。

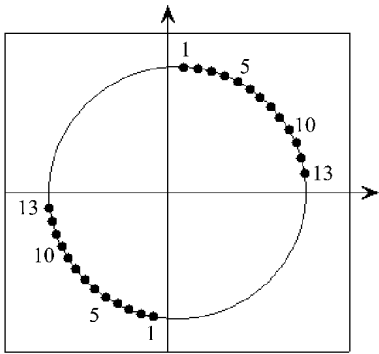


图 2 DFT 域 (对称性) 嵌入模板

Fig 2 Embedding template (symmetrically) in DFT domain

2.2 基于图像大小的重同步

本文通过登记原始图像的大小, 可以使得水印图像重定大小。从而水印可以抵抗图像的缩放、长宽比改变攻击, 并和二维交织、BCH 技术一起可以抵抗 jitter、小范围的裁剪等几何攻击。在检测一幅图像是否嵌有水印之前, 首先提取待检测图像中的模板, 主要是在待检测图像 DFT 的幅度值半径为 R 的圆周上寻找局部峰值点, 把这些峰值点作为可能的模板点, 然后与原始模板进行比较。由它的变化情况, 来决定待检测图像所遭遇的旋转攻击。最后对待检测图像进行逆旋转, 使其尽可能地重同步于原始图像, 据文 [5] 提取有意义信息。如果检测图像未遭遇的旋转攻击, 则根据登记的原始图像的大小, 重定待检测图像的大小, 然后据文 [5] 提取有意义信息。注意: 在实验中, 图像的重定大小和旋转都采用双线性插值。

由于本文算法只在一个圆周上搜索局部峰值点, 因此搜索空间和同原始模板进行比较的复杂度都很低。对于模板和字符串的嵌入和提取过程, 计算量为小波变换和 FFT 变换的计算量之和。另外二维 DWT 的计算复杂度是 $O(N^2)$, FFT 的计算复杂度是 $O(N^2 \log N)$ (假设原始图像大小为 $N \times N$)。所以该算法的计算复杂度是 $O(N^2 \log N)$ 。

3 实验结果

在纹理复杂性不同的图像“Lena”(512×512×8 bits)和“Baboon”(512×512×8 bits)上测试所提出的算法。2 个测试图像分别嵌入一个 536 bits (67 个字符)的字符串“Dept. of Computer Science, Zhongshan University, Guang Zhou, P. R. China”作为水印,在此基础上再嵌入模板。其中嵌入字符串时,“Lena”图像 S 取 32 (改变 5 bits 位),“Baboon”图像 S 取 64 (改变 6 bits 位);嵌入字符串和模板后的“Lena”图像的 PSNR (peak signal to-noise ratio) 为 43.09 dB,嵌入字符串和模板后的“Baboon”图像的 PSNR 为 37.63 dB。从视觉效果的角度,嵌入字符串和模板前后的“Lena”图像和“Baboon”图像无明显差异(图 3)。模板的参数选择: $R=100$, $Num=13$, $N=5$, $WinLen=3$ 。

表 1—3 给出了所嵌入的模板受 StirMark3.1 攻击后的一些性能。表 1 显示模板受到旋转攻击,模板都能准确地纠正。表 2 显示当 JPEG 压缩的质量

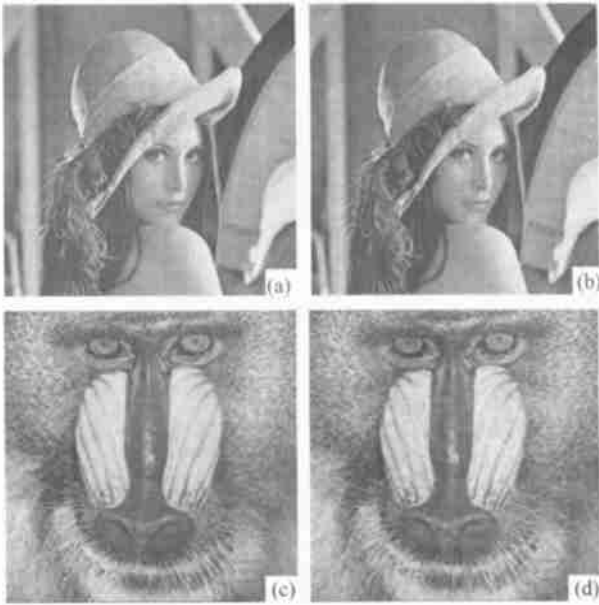


图 3 水印的不可见效果

Fig 3 Demonstration of invisibility
(a) 原始图像; (b) 水印图像 (43.09 dB);
(c) 原始图像; (d) 水印图像 (37.63 dB)

表 1 模板抗 StirMark 3.1 的 Rotation 性能

Tah 1 Template against rotation of StirMark 3.1

旋转角度	90	45	30	15	10	5	−2	1	−0.75	0.5	−0.5	0.25	−0.25
检测结果	90	45	30	15	10	5	−2	1	−0.75	0.5	−0.5	0.25	−0.25

表 2 模板抗 StirMark 3.1 的 JPEG 压缩性能

Tah 2 Template against JPEG compression of StirMark 3.1

JPEG 的质量因子	90	80	70	60	50	40	35	30	25	20	15	10
检测到的模板点个数	13	13	13	13	13	13	13	12	8	4	2	4

表 3 模板抗 StirMark 3.1 的滤波性能

Tah 2 Template against filtering of StirMark 3.1

滤波器的类型	2×2median filter	3×3median filter	4×4median filter	Gaussian filtering
检测到的模板点个数	13	13	13	13

表 4 水印图像抗 StirMark 3.1 性能

Tah 4 Experimental results with StirMark 3.1

StirMark functions	BER(Lena)	BER(Baboon)	StirMark functions	BER(Lena)	BER(Baboon)
jitter, scaling	0	0	rotation-15	3.50	3
cropping-10	0	0	rotation-10	1.10	0.9
cropping-25	4	0	rotation-90, 5, 2, −2	0	0
Gaussian-filtering	0	0	rotation-1, −1, 0.75, −0.5	0	0
aspect ratio change	0	0	rotation −0.75, 0.5	0	0
rotation-45	8.2	11.9	rotation 0.25, −0.25	0	0
rotation-30	7.65	7.3	stir mark random bend	46.08	52.61

因子 (quality factor) 大于 35 的时候, 模板的所有 13 个点都能检测到, 而 quality factor 为 35 的 JPEG 压缩图像的质量已经较差。表 3 显示了模板对于常见滤波的稳定性。

表 4 给出“Lena”和“Baboon”水印图像受 StirMark 3.1 攻击后的性能。其中 BER (bit error rate) 为检测到的信息位错误率。从表 4 中可以看出, 所提出的算法在受到 Stirmark 的 Scaling 攻击和 Rotation (伴随裁剪的旋转) 攻击, 借助于登记原始图像的大小和模板, 通过逆过程, 再用检测算法提取水印, 效果普遍较好, 只有 Rotation 攻击在裁剪过多时有一些误码。本文的算法也可以较好抵御某些行和列的随机抽取, 也称为 jitter 攻击。根据文献 [6, 8], 大多数基于扩频的水印技术都无法抵御 jitter 攻击。为了进行公平的比较, 在文 [6, 8] 中通常考虑在 $256 \times 256 \times 8$ bits 图像中隐藏了 100 bits (有效信息, 已去除了纠错编码引入的冗余位)。而本文提出的算法, 去除图像尺寸的影响, 相当于在 $256 \times 256 \times 8$ bits 图像中隐藏了 $536/4 = 134$ bits。本文的算法还可以抵抗长宽比的变化和小范围的裁剪等攻击。

从表 4 中还可以看出, 水印图像在随机选择加弯曲 (Randomization and Bending) 攻击的情况下, 导致隐藏信息位的严重错误 (许多嵌入的信息位都丢失了), 出现比较大的比特差错率。主要因为嵌入的是有意义信息, 而非随机序列。较大范围的裁剪或弯曲, 容易导致水印信息丢失或无法重同步。当然还有一些攻击本算法无法对抗, 需要进一步研究。

参考文献:

- [1] PEREIRA S, O'RAUANAIDH J J K, DEGUILLAUME F, et al. Template based recovery of Fourier-based watermarks using log-polar and log-log maps // IEEE Int Conf on Multimedia Computing and Systems (ICMCS'99) [C]. Florence, Italy, 1999.
- [2] PEREIRA S, O'RAUANAIDH J J K, PUN T. Secure robust digital watermarking using the lapped orthogonal transform // IST/SPIE Electronic Image '99, Session: Security and Watermarking of Multimedia Contents [C]. San Jose, CA, 1999.
- [3] PEREIRA S, PUN T. Fast robust template matching for affine resistant image watermarks // Proc 3rd Int Information Hiding Workshop [C]. 1999: 207—218.
- [4] O'RAUANAIDH J J K, PEREIRA S. A secure robust digital image watermark // Electronic Imaging: Processing, Printing and Publishing in Colour, SPIE Proceedings [C]. Zürich, Switzerland, 1998.
- [5] 刘九芬. 小波理论及其在图像压缩和数字水印中的应用: 一种盲检测的有意义图像水印算法 [D]. 杭州: 浙江大学, 2001: 87—95.
- [6] PETITCOLAS F A P, KUHN M G. StirMark. <http://www.cl.cam.ac.uk/~fapp2/watermarking/benchmark/>. 1999.
- [7] ELMASRY G F, SHI Y Q. 2-D interleaving for enhance the robustness of watermark signals embedded in still image // Proc of IEEE Int Conf on Multimedia and Expo [C]. 2000.
- [8] PETITCOLAS F A P, ANDERSON R J, KUHN M G. Attacks on copyright marking systems // Proc of the 2nd Int Workshop on Information Hiding, Lecture Notes in Computer Science [C]. Berlin: Springer-Verlag, 1998.

A Meaning Image Watermarking Algorithm

WANG Zhen wu¹, LIU Jiu fen^{2,3}, HUANG Da ren³

(1. Department of Computer Science, Sun Yat sen University, Guangzhou 510275, China;

2. NLPRI, Institute of Automation, Chinese Academy of Science, Beijing 100080, China;

3. Department of Scientific Computing and Computer Applications,
Sun Yat sen University, Guangzhou 510275, China)

Abstract: A watermarking algorithm in DWT domain is proposed. The proposed algorithm hides data as many as 536 bits in $512 \times 512 \times 8$ bits images. And no original images are required in watermark signals' extraction. By means of BCH coding, 2-D interleaving, template, and registration of the width and height of the original image technology, the algorithm is robust against the common signal processing procedures as well as some geometric attacks of StirMark 3.1, such as aspect ratio variation, jitter, rotation, scaling, etc.

Key words: geometric distortion; wavelet transform; meaning watermark; 2-D interleaving; template