

一种实现多个隐形签名的数字水印算法研究

李京兵^{1,2}, 黄席樾¹, 周亚训³

(1. 重庆大学 自动化学院, 重庆 400044; 2. 海南大学 旅游学院, 海南 海口 570228; 3. 宁波大学 电子信息工程系, 浙江 宁波 315211)

摘 要: 给出了一种新的数字水印算法, 并对加有多个水印的图像进行了 JPEG 压缩、加高斯噪声、图像剪切和中值滤波等攻击实验。仿真结果表明用该算法嵌入的多水印有理想的鲁棒性。

关键词: 鲁棒性; 小波变换; 数字图像; 多水印

中图法分类号: TN918 文献标识码: A 文章编号: 1001-3695(2005)08-0252-03

An Algorithm of Multiple Invisible Signatures

LI Jing-bing^{1,2}, HUANG Xi-yue¹, ZHOU Ya-xun³

(1. College of Automation, Chongqing University, Chongqing 400044, China; 2. College of Tourism, Hainan University, Haikou Hainan 570228, China; 3. Dept. of Electronic Information & Engineering, Ningbo University, Ningbo Zhejiang 315211, China)

Abstract: Original image is not required for detecting the invisible signatures, and the signatures can be detected in parallel. Many simulation experiments have been done, such as JPEG compression, noise contamination, medianfiltering and image cropping. The simulation experimental results show that the embedded digital watermarks with the proposed algorithm are robust enough.

Key words: Robustness; DWT; Digital Image; Multiple Watermarks

随着多媒体网络的不断普及, 数字化媒体的传输和获取变得越来越便捷, 如何有效地保护数字图像等各种数字媒体的版权问题变得日益重要。数字水印是数字媒体版权保护的有效手段。但目前对单水印的嵌入与提取研究较多, 而实际中往往需要在数字媒体中嵌入多水印, 如一个数字原件需由多人签名; 一个数字媒体由多道工序完成, 在作品完成后, 由多个制作人签名。因此, 多水印的嵌入与提取有较大的实用价值。用传统的方法进行多水印的嵌入^[1], 由于在宿主图像所嵌入的信息量增多, 水印的鲁棒性和不可见性矛盾日益突出, 并且多水印的提取是按序进行, 这样当嵌入的水印较多时, 提取水印费时较多。为此, 提出了一种基于小波域的嵌入多个隐形签名的数字水印算法, 较好地解决了这一难题。嵌入的每个水印生成相应的一个逻辑表, 这个逻辑表作为一个密钥, 通过向第三方注册, 来保护自己对原作品的所有权^[2]。并且通过这个密钥 (Secret Key) 提取图像中与之对应的水印, 多个水印可以并行提取。在本文中嵌入和提取的水印不是常用的无意义随机序列, 而是有实际意义的签名 (二值图像)。这样水印更形象直观, 便于识别和版权保护。

1 图像的小波变换

S. Mallat 于 1988 年提出的小波变换 (DWT), 是近几年兴起的一个新的信号分析理论, 它是一种“时—频”分析方法, 其基本思想是以小波函数 $\Psi_{a,b}(t)$ 为基底, 对信号 $f(t)$ 进行分解。

$$W_{f(a,b)} = \int_R f(t) \overline{\Psi_{a,b}(t)} dt$$

其中小波函数 $\Psi_{a,b}(t)$ 是由同一基底函数 Ψ 经平移、伸缩而得到的一组函数。

$$\Psi_{a,b}(t) = |a|^{-1/2} \Psi((t-b)/a) \quad a, b \in R, a \neq 0$$

其中 Ψ 称为基小波, a 为伸缩因子, b 为平移因子。

小波变换是一种多分辨分析, 其中常用的 Mallat 算法对信号进行小波分解与重构过程如图 1(a) 和图 1(b)

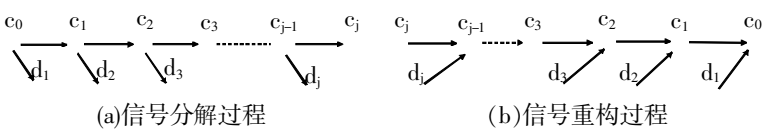


图 1 Mallat 算法信号小波分解与重构过程

Mallat 算法分解公式为

$$c_{j+1,k} = \sum_{n \in Z} c_{j,n} \overline{h_{n-2k}} \quad k \in Z$$
$$d_{j+1,k} = \sum_{n \in Z} c_{j,n} \overline{g_{n-2k}} \quad k \in Z$$

重构公式为 $c_{j,k} = \sum_{n \in Z} c_{j+1,n} h_{n-2k} + \sum_{n \in Z} d_{j+1,n} g_{n-2k} \quad k \in Z$

对二维信号图像进行一级小波分解后, 原图分成四个子图, 其中三个高频细节子图 (水平、垂直和对角线方向) 和一个低频逼近子图。高频细节子图主要包含了原图的边缘信息, 但容易受到外部干扰的影响 (常规的图像处理), 而低频逼近子图包含图像的基本信息 (低频部分), 受外部影响小, 因此把水印加在逼近子图中, 有好的鲁棒性, 把原图进行三级小波分解后, 细节子图为 HH1, LH1, HL1; HH2, LH2, HL2; HH3, LH3, HL3 逼近子图为 LL3, 子图分布如图 2 所示。

LL3	LH3	LH2	LH1 (水平方向)
HL3	HH3		
HL2		HH2	HH1 (对角线方向)
HL1 (垂直方向)			

图 2 原图经过三级小波分解后小波系数分布

新的图像压缩 JPEG2000 和视频压缩标准 MPEG-4 都采用了 DWT。因此选用 DWT 进行水印的制作, 与新的图像和视频压缩标准有较好的兼容性

原始信号选用 Lena(512 ×512 ×8), 经过三级小波分解后, 逼近子图 LL3 受常规图像处理的影响情况(表 1), 表中均

方误差^[3]所用计算公式 $MSE = \frac{1}{MN} \sum_i \sum_j (I_{(i,j)} - I'_{(i,j)})^2$

峰值信噪比 PSNR(dB) 所用公式

$$PSNR = 10 \lg \left[\frac{MN \max_{i,j} (I_{(i,j)})^2}{\sum_i \sum_j (I_{(i,j)} - I'_{(i,j)})^2} \right]$$

其中 $I_{(i,j)}$ 表示原始图像中, 坐标为(i, j) 的像素点的灰度值; $I'_{(i,j)}$ 表示已嵌入水印的图像中, 坐标为(i, j) 的像素点的灰度值; M, N 表示图像的行和列的像素值。

从表 1 中可知干扰前后均方误差 MSE(对 LL3 的所有系数计算得到) 的值很小, 这说明 LL3 系数变化很小。从表 1 中实际观察 LL3 部分系数的变化情况, 可以发现, 整数部分基本不变, 小数部分变化微小(与表中原图的 LL3 相应系数相比), 因此可以将水印信号嵌入在 LL3 的小数部分, 这样既能保证水印的鲁棒性和又不改变细节子图系数, 使原图像边缘清晰。

表 1 三级小波分解后的逼近子图系数受常规图像处理的影响

	PSNR (dB)	PMSE (LL3)	选 LL3 的前 10 个系数实际观察									
			(1, 1)	(1, 2)	(1, 3)	(1, 4)	(1, 5)	(1, 6)	(1, 7)	(1, 8)	(1, 9)	(1, 0)
原图 Lena			5. 178	5. 198	5. 065	5. 027	4. 974	5. 082	5. 147	5. 185	5. 105	5. 210
加高斯噪声	29. 16	0. 001	5. 005	5. 004	5. 144	5. 133	5. 009	5. 108	5. 069	5. 047	5. 056	5. 252
中值滤波	31. 06	0. 02	5. 069	5. 083	5. 026	5. 113	4. 924	4. 978	5. 075	5. 109	5. 072	5. 188
JPEG 压缩	30. 10	0. 005	5. 271	5. 294	5. 132	4. 957	4. 957	4. 933	5. 096	5. 271	5. 271	5. 249

2 数字水印算法

2.1 多水印的嵌入

每个有意义的签名选用一个二值图像, 把它作为要嵌入的数字水印。设嵌入的第 g 个水印为 $W^g = \{ w_{(i,j)}^g \mid w_{(i,j)}^g = 0, 1; 1 \leq i \leq M_1, 1 \leq j \leq M_2 \}$, 原始图像选为 lena(512 ×512 ×8), 原始图像记为 $F = \{ f_{(i,j)} \mid f_{(i,j)} \in R; 1 \leq i \leq N_1, 1 \leq j \leq N_2 \}$ 其中 $w_{(i,j)}^g$ 和 $f_{(i,j)}$ 分别表示第 g 个二值水印图像和原始图像的像素灰度值, 这里设 $M_1 = M_2 = M, N_1 = N_2 = N$, 水印的嵌入分如下几步:

(1) 对原图进行小波 L 级分解并获得逼近子图系数的小数部分 FAD_L 。

对原始图像进行 L 级小波分解后, 可以得到多个细节子图系数 $FD_j^k (k = 1, 2, 3; j = 1, 2, 3, \cdots, L)$ 和一个逼近子图系数 FA_L , 那么逼近子图系数的小数部分 $FAD_L(i, j) = FA_L(i, j) - \text{floor}(FA_L(i, j))$, 式中 $\text{floor}()$ 函数是向下取整函数, 小波分解级数 $L \leq \text{floor}(\log_2(N/M))$, 分解级数高, 鲁棒性较好, 但小波分解和重构时间相应加长, 这里取等号。

(2) 将多个水印 $w^g(i, j), (g = 1, 2, 3)$, 嵌入逼近子图小数部分, 并生成与水印相关的逻辑表 $key^g(i, j), (g = 1, 2, 3)$ 。

为了使得嵌入的水印有较好的鲁棒性和不可见性, 充分考虑了原图逼近子图的小数部分 $FAD_L(i, j)$ 的大小, 当 $0 \leq FAD_L(i, j) < 0.5$ 时, 取中值 0.25, 当 $0.5 \leq FAD_L(i, j) < 1$ 时, 取中值 0.75。

```
if 0 ≤ FADL( i, j) < 0. 5 then
FADL( i, j) = 0. 25
keyg( i, j) = XOR( wg( i, j) , 0)
else if 0. 5 ≤ FADL( i, j) < 1 then
```

```
FADL( i, j) = 0. 75
keyg( i, j) = XOR( wg( i, j) , 1)
end
```

生成的二值逻辑表 $key^g(i, j)$ 包含了水印 $w^g(i, j)$ 的信息, 保存 $key^g(i, j)$, 在下面提取相应的水印要用到, 可将 $key^g(i, j)$ 作为密钥向第三方申请, 以获得原作品的所有权^[2]。

(3) 组合生成新的逼近子图系数 $FA'_L(i, j)$ 。

$FA'_L(i, j)$ 由逼近子图系数的整数部分 $\text{floor}(FA_L(i, j))$ 和加了水印信息的逼近子图系数的小数部分 $FAD_L(i, j)$ 组合而成。

$FA'_L(i, j) = \text{floor}(FA_L(i, j)) + FAD_L(i, j)$

2.2 多水印的提取

(1) 求出逼近子图的小波系数的小数部分 $T_FAD_L(i, j)$ 。

对待测图像 $Test_F$ (简记为 T_F) 进行 L 级小波分解, 求出逼近子图的小波系数 $T_FAD_L(i, j)$ 的小数部分 $T_FAD_L(i, j)$ 。

$T_FAD_L(i, j) = T_FA_L(i, j) - \text{floor}(T_FA_L(i, j))$

(2) 多水印的提取。

根据嵌入的水印生成的逻辑表 $key^g(i, j), (g = 1, 2, 3)$ 和含水印信息的逼近子图小波系数的小数部分, 求出嵌入的相应水印 $w^{*g}(i, j)$ 。提取水印方法如下:

```
if 0 ≤ T_FADL( i, j) < 0. 5 then
w*g( i, j) = XOR( keyg( i, j) , 0)
else if 0. 5 ≤ FADL( i, j) < 1 then
w*g( i, j) = XOR( keyg( i, j) , 1)
end
```

根据多个水印在嵌入时生成的多个逻辑表 $key^g(i, j), (g = 1, 2, 3)$, 在提取水印时, 可以提取出对应的多个水印 $w^{*g}(i, j), (g = 1, 2, 3)$ 。而且多水印的提取不需要原始图像。有利于保护原始图像的安全, 多水印的提取可以并行进行。

3 仿真实验

仿真平台为 MATLAB 6. 1, 仿真中原始图像选为 Lena (512 ×512 ×8), 对其进行三级小波分解, 小波选用的是 Daubechies 正交小波 ‘db2’。三级分解后, 逼近子图系数 LL3 系数矩阵大小为 66 ×66 点阵, 而嵌入的每个水印大小为 33 ×33, 因此在具体编程时, 一个水印可嵌入四次, 提取时取平均值, 这样可进一步提高水印的鲁棒性。

图 3(a) 是原始图像, 图 3(b) 是嵌入水印后的图像 ($PSNR = 34.98$), 在视觉上与原图基本上没有什么变化, 满足水印的不可见性的要求, 图 3(c) 为检测到的三个嵌入的水印。当没有受到攻击时, 水印检测的误码率为 $P_{b1} = P_{b2} = P_{b3} = 0$

下面通过实验, 测试该多水印算法的鲁棒性:

(1) 加入噪声

使用 $\text{imnoise}()$ 函数加入高斯噪音。当噪声强度为 3. 0% 时, 这时 $PSNR$ 降至 15. 5dB, 加有水印的图像在视觉上已很模糊见图 4(a) , 图像退化已很严重, 但通过图 4(b) 可以看到, 提取的水印仍较清晰, 三个水印对应的误码率分别为 $P_{b1} = 3. 77\%, P_{b2} = 4. 41\%, P_{b3} = 3. 67\%$ 。通过表 2 的实验数据可以看到, 当高斯噪声强度为 4% 时, $PSNR$ 降至 14. 4dB, 这时检测的三个水印的误码率分别是 $P_{b1} = 7. 16\%, P_{b2} = 7. 62\%, P_{b3} = 7. 16\%$ 仍能检测出水印的存在。这说明采用该算法嵌入的多水

印有理想的抗高斯噪声能力。



图 3 水印嵌入与检测

表 2 多个水印抗高斯噪声实验数据

噪声强度 (%)	0	1	2	3	4
$PSNR$ (dB)	34. 9	19. 9	17. 1	15. 5	14. 4
P_{b1} (%)	0. 00	0. 09	0. 83	3. 77	7. 16
P_{b2} (%)	0. 00	0	0. 83	4. 41	7. 62
P_{b3} (%)	0. 00	0. 09	1. 29	3. 67	7. 16

(2) 滤波处理

采用[5 ×5] 中值滤波, 重复 20 次后($PSNR = 26. 38\text{dB}$), 这时含水印的图像为图 5(a) , 图像边缘已不太清晰, 其水印检测见图 5(b) , 明显的检测到三个水印的存在, 并有较低的误码率, $P_{b1} = 2. 29\%$; $P_{b2} = 2. 11\%$; $P_{b3} = 1. 74\%$ 。通过表 3 的具体数据可以看到, 经多次的中值滤波(0 ~20 次) , 都有较低的误码率。这说明该算法有较强的抗中值滤波攻击能力。



图 4 多水印抗高斯噪声结果
($PSNR=15.5$)

图 5 多水印抗重复滤波
实验结果

表 3 多水印抗重复滤波实验数据

滤波次数	0 次	5 次	10 次	15 次	20 次
$PSNR$ (dB)	34. 98	28. 17	27. 20	26. 72	26. 38
P_{b1} (%)	0	0. 37	1. 19	1. 88	2. 29
P_{b2} (%)	0	0. 37	1. 38	1. 79	2. 11
P_{b3} (%)	0	0. 51	1. 10	1. 38	1. 74

(3) JPEG 压缩处理

采用图像质量百分数作为参数对含水印的图像进行 JPEG 压缩实验, 图 6(a) 是压缩质量为 4% ($PSNR = 26. 18\text{dB}$) , 图像视觉质量较差, 已有由压缩而产生的方块效应, 通过图 6(b) 可以看到该算法仍能检测到三个水印的存在($P_{b1} = 3. 21$, $P_{b2} = 2. 57$, $P_{b3} = 2. 84$) 。通过表 4 的具体实验数据可以发现, 当压缩质量大于 6% 后, 误码率都基本不变, 并保持较低的值。这说明该算法有很理想的抗 JPEG 压缩能力。

表 4 多个水印抗 JPEG 压缩实验数据

压缩质量 (%)	2	4	6	8	10
$PSNR$ (dB)	24. 29	26. 18	27. 52	28. 59	29. 23
P_{b1} (%)	28. 28	3. 21	0. 28	0	0
P_{b2} (%)	28. 01	2. 57	0. 09	0	0
P_{b3} (%)	25. 53	2. 84	0. 09	0	0

(4) 几何切割

图 7(a) 表示几何切割面积为 40% 时的含水印图像, 这时的 $PSNR = 9. 04\text{dB}$ 。通过图 7(b) 看到检测到的水印, 误码率分别为 $P_{b1} = 4. 68$, $P_{b2} = 3. 77$, $P_{b3} = 3. 77$ 。通过表 5 的具体实验数据可以发现当切割面积高达 50% , 仍能检测出水印的存在,

这时 $P_{b1} = 5. 23$, $P_{b2} = 4. 32$, $P_{b3} = 4. 32$ 。这说明该算法对几何切割也有较好的抗攻击能力。



图 6 多水印抗 JPEG 压缩实验结果

图 7 多水印抗几何失真实验结果

表 5 多水印抗图像切割的实验数据

切割比例 %	10	20	30	40	50
$PSNR$ (dB)	15. 37	12. 38	10. 33	9. 04	8. 19
P_{b1} (%)	0	1. 65	4. 87	4. 68	5. 23
P_{b2} (%)	0	0. 92	3. 86	3. 77	4. 32
P_{b3} (%)	0	0. 28	3. 12	3. 77	4. 32

通过以上几个实验结果和详细的实验数据表明, 采用该算法嵌入的多水印对常见的图像操作有较强的鲁棒性, 在经过比较严重的攻击后, 仍能检测出三个水印的存在。

4 结论

本文提出了基于小波域多个隐形签名水印嵌入与检测算法。通过实验验证了其理想的鲁棒性和不可视性, 较好地解决了在水印嵌入时, 鲁棒性和不可视性的矛盾, 多水印可以并行提取, 并且水印提取不需要原始数字图像, 有较高的实用价值。该多水印算法不仅能用于数字图像的版权保护, 还能用于数字音频、数字视频等其他数字媒体的版权保护, 为多个隐形签名研究开辟了一条新的思路。

参考文献:

[1] Cox I J Kilian, *et al.* Secure Spread Spectrum Watermarking for Multimedia[J] . IEEE Trans. Image Processing, 1997, 6 (12) : 1673-1687.

[2] Pan Jeng-Shyang, *et al.* A VQ-based Multi-Watermarking Algorithm [R] . Proceedings of IEEE TENCON , 2002. 117-1206.

[3] 王炳锡, 等. 数字水印技术[M] . 西安: 西安电子科技大学出版社, 2003. 82-83.

[4] 周亚训, 叶庆卫, 等. 基于二值运算的数字图像水印嵌入与检测算法[J] . 计算机辅助设计与图形学学报, 2002, 14(2) : 148-152.

[5] Mallat S. A Theory of Multiresolution Signal Decomposition: The Wavelet Representation[J]. IEEE Trans. on PAMI, 1989, 11(7) : 674-693.

[6] Wong P H W, *et al.* A Novel Blind Multiple Watermarking Technique for Images[J] . IEEE Transaction on Circuits and Systems for Video Technology, 2003, 13(8) : 813-830.

[7] Wong P H W, Au O C. A Blind Watermarking Technique for Multiple Watermarks[R] . Proceeds of International Symposium on Circuits and Systems, 2003. 936-939.

作者简介:

李京兵(1966-) , 男, 河北邯郸人, 副教授, 在读博士, 主要研究方向为网络技术、图像处理、信息隐藏等; 黄席樾(1943-) , 男, 四川奉节人, 教授, 博士生导师, 主要研究方向为复杂系统控制理论及智能机器人学等; 周亚训(1965-) , 男, 浙江宁波人, 副教授, 在读博士, 研究方向为数字信号、图像处理、光纤通信等。