基于关键点信息的鲁棒参考水印算法

佘 昆[1,2], 黄均才[1,2,3], 周明天[1,2]

(1. 电子科技大学计算机学院, 四川成都 610054; 2. 电子科技大学2卫士通联合实验室, 四川成都 610054;
3. 华东交通大学经管学院, 江西南昌 330013)

摘 要: 鲁棒参考水印(RRW)算法是基于小波多分辨分析的用于静态图像的数字水印算法, 在分析了 RRW 算法在图像小波分解系数的平均值较小时的缺陷的基础上, 根据人眼视觉原理, 提出了利用水印的关键点信息来改进 RRW 算法的思想. 与常规 RRW 算法不同, 算法使用关键点信息, 在对小波系数进行特征量化时, 对关键点取较小的 Q 值, 对非关键点取较大的 Q 值. 在水印检测中, 对关键点和非关键点赋予不同的权值, 并深入分析了该方法的正向错误概率和负向错误概率的计算公式. 实验结果表明, 改进算法不但其性能优于原算法, 而且还在一定程度上缓解了水印的不可见性和健壮性之间的矛盾.

关键词: 数字水印; 鲁棒参考水印; 关键点

中图分类号: TP391 文献标识码: A 文章编号: 0372-2112 (2003) 11-1709-04

Robust Reference Watermarking Algorithm Based on Key Points

SHE Kun[1,2], HUANG Jun-cai[1,2,3], ZHOU Ming-tian[1,2]

(1. College of Computer Sci&Engineering, Univ. of Electronic Sci&Tech of China, Chengdu, Sichuan 610054, China;
2. Information Security United Lab. of UESTC-Westone, Chengdu, Sichuan 610054, China;
3. College of Eco&Management, East China Jiaotong University, Nanchang, Jiangxi 330013, China)

Abstract: Robust Reference Watermarking(RRW) is a digital watermarking algorithm of still images based on the concept of multiresolution wavelet fusion. The concept of "Key points" is applied to watermarking in order to improve the robustness of RRW. Normal RRW uses only a constant Q to quantize wavelet coefficient. In the quantization process of improved method, if the watermark point is key point, then use larger quantizing parameter Q to quantize wavelet coefficient, else use smaller Q. When detecting watermark, key points' weight value are 1, and others' are constant not smaller than 0 and not larger than 1. Analysis is provided to compute the probability of false positive and false negative results. Experimental results show the performance of our method is better than the original RRW method and demonstrate its potential for the robust watermarking of photographic imagery.

Key words: digital watermark; robust reference watermarking; key point

1 引言

数字水印是保护多媒体数据版权的有效方法, 它通过在原始图像数据中嵌入某些私有信息))) 水印(Watermark)来判定图像的所有权归属.

水印的基本要求是不可见性和健壮性(鲁棒性), 但二者往往是相互矛盾的, 研究水印算法就是要在保证不可见性的前提下, 尽可能多地嵌入水印.

水印可分为空域/时域水印和变换域水印. 与空域/时域水印相比, 变换域水印的健壮性更强, 因而得到了广泛的重视. 数字水印技术中常用到的变换主要是离散余弦变换(DCT)和离散小波变换(DWT), 相应的水印技术称为离散余弦变换域水印[1~3]和离散小波变换域水印[4~6].

Deepa Kundur[7]等人将水印的添加和提取结合起来考虑, 提出了鲁棒参考水印(Robust Reference Watermarking, RRW)算法. 该算法用了两种水印, 即鲁棒水印和参考水印, 两者相互正交, 它们被同时添加到经过 DWT 后的载体图像小波系数中. 但 Deepa Kundur 方法在嵌入、提取和检测水印信息时对水印信息的各点不加以区分, 导致在某些情况下算法失效. 我们通过引入关键点的概念, 在嵌入、提取和检测水印信息时对水印信息的关键点和非关键点作不同处理, 改进了 RRW 算法, 从整体上提高了水印的性能, 并在一定程度上克服了不可见性和健壮性之间的矛盾.

2 原鲁棒参考水印算法描述

Deepa Kundur 提出的鲁棒参考水印算法对于水印的添加位置依赖于原始图像和所选择的密钥, 并且检测时不需要原图信息.

收稿日期: 2003-01-08; 修回日期: 2003-07-23
基金项目: 电科院基金(No. JD05972)

2.1.1 RRW 算法介绍

假设水印 $w(i,j)$ 是长度为 N_w, 由 1 和 -1 组成的一个序列, 并假定原始载体图像为 f, 则水印的嵌入过程如图 1 所示, 设 DWT 变换的第 l 级 ($l=1,\cdots,L$) 细节系数为 $f_{k1,l}(ic,jc)$、$f_{k2,l}(ic,jc)$、$f_{k3,l}(ic,jc)$, 其中 k1, k2, k3 $\in$ {H, V, D}, 分别表示水平、垂直和对角线细节系数. 若位置 (ic,jc) 需要嵌入水印数据, 则对小波细节系数进行排序, 使得 $f_{k1,l}(ic,jc) \geqslant f_{k2,l}(ic,jc) \geqslant f_{k3,l}(ic,jc)$. 对 $f_{k1,l}(ic,jc)$ 和 $f_{k3,l}(ic,jc)$ 间的值进行分段:

$$\$ = \frac{f_{k3,l}(ic,jc) - f_{k1,l}(ic,jc)}{2Q-1} \tag{1}$$

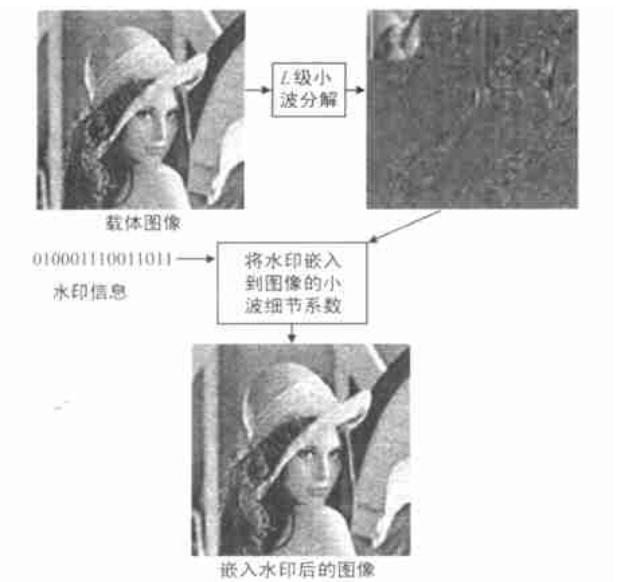

图 1 RRW 嵌入水印过程

然后对 $f_{k2,l}(ic,jc)$ 进行量化, 量化过程如图 2 所示.

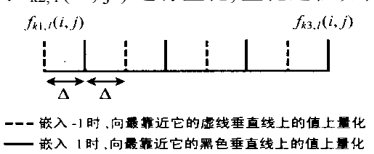

图 2 量化过程

提取水印时对待测图像 $r(i,j)$ 的细节系数 $r_{k1,l}(ic,jc)$, $r_{k2,l}(ic,jc)$, $r_{k3,l}(ic,jc)$ 进行排序, 使得 $r_{k1,l}(ic,jc) \geqslant r_{k2,l}(ic,jc) \geqslant r_{k3,l}(ic,jc)$, 采用与嵌入水印时使用的相同 Q 值来进行分段, 寻找与 $r_{k2,l}(ic,jc)$ 最接近的量化值, 以确定嵌入的是 1 还是 -1.

水印的检测采用将原始水印与提取出的水印作相关, 再与阈值 T 进行比较来进行. 相关用下述公式进行计算:

$$Q(w,w') = \frac{\sum w(i,j)w'(i,j)}{\sqrt{\sum w^2(i,j)}\sqrt{\sum w'^2(i,j)}} \tag{2}$$

其中 w 代表原始水印, w′ 代表提取出的水印.

阈值 T 的确定与正向错误 (虚警) 概率和负向错误 (漏报) 概率有关. 定义正向错误概率为

$$P_{fp} = P(Q(w,w') \geqslant T \mid \text{无水印}) \tag{3}$$

则可推导得 P_{fp} 的计算公式为

$$P_{fp} = \sum_{m=7N_w(T+1)/2}^{N_w} \binom{N_w}{m} 0.5^{N_w} \tag{4}$$

定义负向错误概率为

$$P_{fn} = P(Q(w,w') < T \mid \text{水印 } w \text{ 被嵌入}) \tag{5}$$

则也可推导得 P_{fn} 的计算公式为

$$P_{fn} \approx \sum_{m=0}^{7N_w(T+1)/2-1} \binom{N_w}{m} \left[\frac{2Q-1}{Q}\operatorname{erfc}\left(\frac{\bar{\$}}{4R}\right)\right]^{N_w-m} \left[1-\frac{2Q-1}{Q}\operatorname{erfc}\left(\frac{\bar{\$}}{4R}\right)\right]^{m} \tag{6}$$

此处 $\bar{\$}$ 为给定图像小波分解系数的 $\$ 的平均值, $\operatorname{erfc}(z) = \frac{2}{\sqrt{\pi}}\int_z^{\infty} e^{-u^2}du$ 为余概率积分.

上面的 Q 值是由使用者确定的变量, Q 越大, 量化层次越多, 视觉降质的可能性越小, 而水印的提取越不精确; Q 越小, 量化层次越少, 水印的提取越精确, 而视觉降质的可能性越大.

2.1.2 RRW 算法的缺陷

理论上, RRW 算法能够经受各种图像攻击, 但这也是有条件的, 即原始图像的小波分解的水平、垂直、对角线细节系数之间的差值的平均值不能太小. 实际上, 因 Q 是常量, 如果修改小波分解细节系数, 使其差值普遍偏小, 如图 3(c), 由于 $\$ 很小, 这时小波变换、小波逆变换以及干扰所引起的误差使得水印的提取很不准确, 从而导致水印检测失败, 如图 3(e).

图 3 RRW 在小波细节系数差值普遍偏小时失效

3 使用关键点信息的改进算法

经过对水印图像的仔细分析, 我们发现人眼在辨别水印时水印信息的各点的影响并不是平均的, 前后发生变化的点 (我们称其为关键点) 对人眼影响最大, 为此, 我们利用水印的关键点对 RRW 作了如下改进:

首先定义关键点,

定义 1　设 w(i,j) 为水印图像的(i,j) 点的编码值(w(i, j) I {1,- 1}),若 w(i,j) 满足下列条件中的任何一个则为关键点:

(1) w(i,j)# w(i? 1,j) = - 1;

(2) w(i,j)# w(i,j? 1) = - 1;

(3) w(i,j)# w(i? 1,j? 1) = - 1;

(4) w(i,j)# w(i? 1,j° 1) = - 1.

则 w(i,j) 为非关键点.

嵌入水印时,采用如下公式计算 $:

$$\$ = \begin{cases} \dfrac{f_{k3,1}(ic,jc) - f_{k1,1}(ic,jc)}{2Q_1 - 1}, & \text{若 } w(i,j) \text{为关键点} \\ \dfrac{f_{k3,1}(ic,jc) - f_{k1,1}(ic,jc)}{2Q_2 - 1}, & \text{若 } w(i,j) \text{为非关键点} \end{cases} \tag{7}$$

其中 $Q_1 < Q_2$,例如, $Q_1 = 2$, $Q_2 = 4$. 其余的嵌入操作同原算法.

提取水印时,若相应位置为关键点,采用与嵌入水印时使用的相同 Q_1 值来进行分段,寻找与 $r_{k2,1}(ic,jc)$ 最接近的量化值,以确定嵌入的是 1 还是- 1. 若相应位置为非关键点,采用与嵌入水印时使用的相同 Q_2 值来进行分段,寻找与 $r_{k2,1}(ic,jc)$ 最接近的量化值,以确定嵌入的是 1 还是- 1.

水印的检测仍然采用将原始水印与提取出的水印作相关,再与阈值 T 进行比较来进行. 不过,为突出关键点对水印检测的影响,我们在计算相关性时对关键点与非关键点赋以不同的权值.

定义 2　设 w(i,j) 为水印图像的(i,j) 点的编码值(w(i, j) I {1,- 1}), A(i,j) 为水印图像的(i,j) 点的权值,若 w(i, j) 为关键点,令 A(i,j) = 1;若 w(i,j) 为非关键点,则 A(i,j) = A,且 0[A[1.

4　水印检测分析

如果采用改进算法,则原始水印与提取出的水印之间的相关性用下述公式进行计算:

$$Q(w,w) = \frac{\mathop{E}\mathop{E} A(i,j)\,w(i,j)\,w(i,j)}{\sqrt{\mathop{E}\mathop{E} A(i,j)\,w^2(i,j)}\ \sqrt{\mathop{E}\mathop{E} A(i,j)\,w^2(i,j)}} \tag{8}$$

因 $w^2(i,j) = w^2(i,j) = 1$,故有

$$Q(w,w) = \frac{\mathop{E}\mathop{E} A(i,j)\,w(i,j)\,w(i,j)}{\mathop{E}\mathop{E} A(i,j)} \tag{9}$$

设水印信息长度为 N_w,其中关键点有 n 个,则非关键点的个数为 $(N_w - n)$,从而 $\mathop{E}\mathop{E} A(i,j) = n + (N_w - n)A$. 若定义 $k(i,j) = w(i,j)\,w(i,j)$,则 $k(i,j) = -1$ 表示解码出错, $k(i,j) = 1$ 表示解码正确,故相关性公式可以进一步写为

$$Q(w,w) = \frac{\mathop{E}\mathop{E} A(i,j)\,k(i,j)}{\mathop{E}\mathop{E} A(i,j)} = \frac{\mathop{E}\mathop{E} A(i,j)\,k(i,j)}{n + (N - n)A} \tag{10}$$

将式(10) 代入式(3) 得

$$P_{fp} = P\left\{ \mathop{E}\mathop{E} A(i,j)\,k(i,j) \setminus (n + (N_w - n)A)T \,\middle|\, \text{no wm} \right\} \tag{11}$$

因为 $k(i,j)$ I $\{1,-1\}$,所以 $\mathop{E}\mathop{E} A(i,j)\,k(i,j)$ 必然在集合

{{ $-(n + (N_w - n)A), -(n + (N_w - n)A) + 2A,$
$-(n + (N_w - n)A) + 2, -(n + (N_w - n)A) + 2A + 2, , ,$
$-(n + (N_w - 3n)A), , , n - (N_w - n)A, , ,$
$n + (N_w - n)A - 2, n + (N_w - n)A - 2A,$
$n + (N_w - n)A$ }

中取值,或表示为

$$\mathop{E}\mathop{E} A(i,j)\,k(i,j) = -(n + (N_w - n)A) + 2hA + 2m \tag{12}$$

其中 h 表示解码正确的非关键点数, m 表示解码正确的关键点数,由此得到

$$P_{fp} = P\left\{ \mathop{E}\mathop{E} A(i,j)\,k(i,j) \setminus (n + (N_w - n)A)T \,\middle|\, \text{no wm} \right\} = \sum_{h=0}^{N_w - n} \sum_{m=m_0}^{n} \left(P(n,m) \# P\left(N_w - n, h\right) \right) \tag{13}$$

其中, $m_0 = 7(n + (N_w - n)A)\#(T + 1)/2 - hA\hat{o}$, $P(N_w - n, h)$ 表示 $(N_w - n)$ 个非关键点中有 h 个点解码正确($k(i,j) = 1$)和 $(N_w - n - h)$ 个解码错误($k(i,j) = -1$)的概率, $P(n,m)$ 表示 n 个关键点中有 m 个点解码正确($k(i,j) = 1$)和 $(n - m)$ 个解码错误($k(i,j) = -1$)的概率,即

$$P(n,m) = \binom{n}{m} P_{E_1}^{n-m} (1 - P_{E_1})^m \tag{14}$$

P_{E_1} 为关键点 (i,j) 的 $k(i,j) = -1$ 的概率,在没有嵌入水印 wm 的情况下, 1 和- 1 出现的概率相等,所以 $P_{E_1} = 0\,1\,5.$

而　$P(N_w - n) = \binom{N_w - n}{h} P_{E_2}^{N_w - n - h} (1 - P_{E_2})^h$ (15)

P_{E_2} 为非关键点 (i,j) 对应的 $k(i,j) = -1$ 的概率,同样在没有嵌入水印 wm 的情况下, 1 和- 1 出现的概率相等,所以 $P_{E_2} = 0\,1\,5.$ 故

$$P(n,m) = \binom{n}{m} P_{E_1}^{n-m} (1 - P_{E_1})^m = \binom{n}{m} 0.5^n \tag{16}$$

$$P(N_w - n, h) = \binom{Nw - n}{h} 0.5^{N_w - n} \tag{17}$$

将式(16) 和式(17) 代入式(13) 即得到当 $Q(w,w) \setminus T$ 时,认为水印不存在的正向错误的概率计算公式为

$$P_{fp} = \sum_{h=0}^{N_w - n} \sum_{m=m_0}^{n} \left(P(n,m) \# P\left(N_w - n, h\right) \right) = \sum_{h=0}^{N_w - n} \sum_{m=m_0}^{n} \left[\binom{n}{m} 0.5^n \right] \# \left[\binom{N_w - n}{h} 0.5^{N_w - n} \right] \tag{18}$$

其中. 如果我们能用系数为 R^2 的白高斯噪声来模拟提取出的水印所受的干扰,采用相似的推导,可得负向错误概率的计算公式

$$P_{fn} U \sum_{h=0}^{N_w - n} \sum_{m=m_0}^{n} (pc(n,m) \# Pc(N_w - n, h))$$

$$= \sum_{h=0}^{N_w-n}\sum_{m=m_0}^{n}\left(\binom{n}{m}\left[\frac{2Q_1-1}{Q_1}\mathrm{erfc}\left(\frac{\$}{4R}\right)\right]^{n-m}\right.$$
$$\#\left[1-\frac{2Q_1-1}{Q_1}\mathrm{erfc}\left(\frac{\$}{4R}\right)\right]^{m}$$
$$\#\left(\binom{N_w-n}{h}\left[\frac{2Q_2-1}{Q_2}\mathrm{erfc}\left(\frac{\$}{4R}\right)\right]^{N_w-n-h}\right.$$
$$\left.\#\left[1-\frac{2Q_2-1}{Q_2}\mathrm{erfc}\left(\frac{\$}{4R}\right)\right]^{h}\right) \quad (19)$$

其中 $m_0 = 7(n + (N_w - n)A)\#(T + 1)/2 - hA\hat{6}$.

当 A= 1 时, n= N_w, 这时可以验证, P_{fp}, P_{fn}退化为原算法的形式, 即原算法可看成改进算法的一种特例.

这样, 在嵌入非关键点时因 Q_2 较大, 量化层次较多, 视觉降质的可能性较小, 虽然提取不精确, 但其权值小, 故对水印的检测影响较小; 在嵌入关键点时因 Q_1 较小, 量化层次较少, 水印的提取精确, 虽然其视觉降质的可能性增加, 但因关键点在整个水印图像中所占比例较少, 故总体影响不大. 从而缓解了水印的不可见性和健壮性之间的矛盾.

5 测试结果

我们采用一幅二值图像图 3(b)作为水印, 载体图像采用 512@512 的彩色 Lena 图像, 如图 3(a). 算法中令 Q_2= Q= 4, Q_1= 2, A= 0.5, 小波采用/ Daubechies2100 小波基, 水印嵌入到载体图像的蓝色分量中, 获得测试结果如图 4 所示.

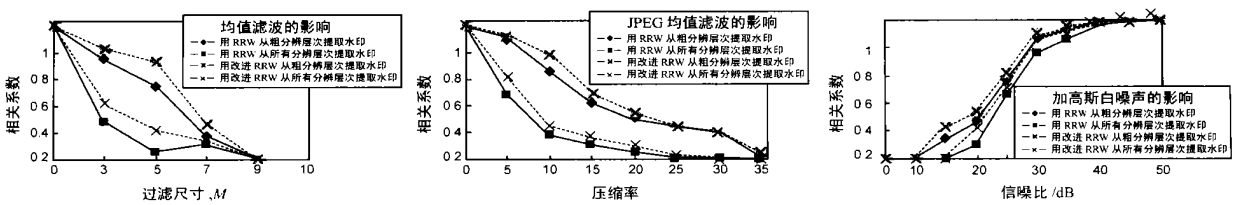

图 4 线性均值滤波、JPEG 压缩及高斯白噪声的测试结果

6 小结

本文在分析原鲁棒参考水印算法的优点和缺陷的基础上, 提出了利用水印的关键点信息来改进鲁棒参考水印算法的思想, 文章还特别在水印检测中为不同性质的水印点赋以不同的权值, 并深入分析了水印检测所依赖的数学依据. 实验表明, 改进算法在提高水印的健壮性的同时并没有显著降低水印的不可见性, 从而在一定程度上缓解了水印的不可见性和健壮性之间的矛盾.

参考文献:

[1] C J Hsu, J L Wu. Hidden Signatures in Images[P]. ICIP2 1996, 223-226.

[2] A G Bors, I Pitas. Embedding parametric digital signatures in images [A]. EUSIPCO. 96[C]. Trieste, Italy, 1996, 9. 1701- 1704.

[3] J Cox. Secure spread pectrum watermarking for multimedia[J]. IEEE Transon Image Processing, 1997, 6(2): 673- 1687.

[4] Houng2Jyh Mike Wang, C2C Jay Kuo. An integrated progressive image coding and watermark system[J]. IEEE Speech and Signal Processing, Seattle, Washington, 1998, 3: 12- 15.

[5] X Xia, C G Boncelet, GR Arce. A multiresolution watermark for digital images[J]. Proc. of IEEE ICIP, Santa Barbara, CA, USA, 1997, 10: 548 - 551.

[6] Rakesh Dugad, K Ratakonda, N Ahuja. A new wavelet2based scheme for watermarking images[A]. IEEE Image Processing, ICIP. 98[C]. Chicago, IL, USA, 1998, 10. 4- 7.

[7] D Kundur, D Hatzinakos. Digital watermark using multiresolution wavelet decomposition[A]. IEEE Intenational Conference On Acous2tics, Speech and Signal Processing[C]. Seattle, Washington, 1998. 2969- 2972.

作者简介:

佘 男, 1967 年 12 月生于湖北武汉, 博士研究生, 主要从事信息安全、中间件计算、电子商务、电子政务的研究工作.

黄均才 男, 1973 年 3 月生于重庆市綦江县, 硕士研究生, 主要从事网络计算、信息安全、生物信息学的研究工作.

周明天 男, 1939 年 3 月生于广西玉林市, 教授, 博士生导师, 主要从事计算机网络、信息安全、并行分布处理等的研究工作.