# 一种改进的小波系数差异量化水印算法

胡 青[1,2] 龙冬阳[1] 卢 伟[1]
(中山大学信息科学与技术学院 广州 510275)[1] (中山大学数学与计算科学学院 广州 510275)[2]

**摘 要** 针对Lin等提出的"基于小波系数差异化量化"(SDQ)的水印方法存在的问题,提出了一种改进的小波系数差异量化水印算法。算法在密钥的控制下,伪随机地选择中频子带中的两块共8个系数组成一组,嵌入1bit水印信息,显著提高了SDQ算法的安全性。算法改进了SDQ的差异量化方式,在保持图像原有的重要系数大小关系的基础上,通过对最大系数进行小幅度的量化来加强差异,进而提高鲁棒性,并通过差异信息和水印信息生成密钥来提取水印。实验结果表明,该算法能有效抵抗各种攻击,并且图像峰值信噪比可以保持在55dB左右。

**关键词** 小波系数,重要系数,重要差异,数字水印

## Improved Watermarking Based on Significant Difference of Wavelet Coefficient Quantization

HU Qing[1,2] LONG Dong-yang[1] LU Wei[1]
(School of Information Science and Technology, Sun Yat-Sen University, Guangzhou 510275, China)[1]
(School of Mathematics and Computational Science, Sun Yat-Sen University, Guangzhou 510275, China)[2]

**Abstract** In this paper an improved SDQ watermarking scheme was developed based on "Significant Difference of Wavelet coefficient Quantization" (SDQ) by Lin et al. Firstly, two blocks of the middle frequency band in DWT were divided into a group of 8 wavelet coefficients in a pseudorandom manner using a key. Then, 1 bit watermark information was embedded in a group. The important coefficients difference was enhanced through slight quantization of the maximum coefficient, and the robustness was improved. Watermark was extracted by a secret key generated by coefficients difference and watermark. The experimental results show that the proposed scheme is quite effective against JPEG compression, low-pass filtering, Gaussian noise and slight geometric attacks, and the PSNR of watermarked image is about 55dB.

**Keywords** Wavelet coefficient, Important coefficients, Significant difference, Digital watermarking

## 1 引言

数字水印是一种在图像中隐藏秘密信息的手段,任何人如果没有密钥,既不能去除嵌入信息,也不能对其解码而进行提取[1]。由于小波变换良好的时频局部性,以及它在压缩标准JPEG2000和MPEG4中的作用,使得基于小波变换域的水印算法成为研究的热点。文献[2]基于小波图像编码中的树结构,提出了超级树概念,通过量化超级树包含的小波系数的低位平面数据来嵌入水印信息。但此方法嵌入的水印信息很容易被擦除,且不能抵抗低通滤波处理。文献[3]针对文献[2]的缺点提出将小波树包含的小波系数的幅值之和看成树的能量,多棵小波树组成一棵超级树。为了防止对应的两棵超级树的能量差别太大,使得系数修改过大,从而导致图像质量严重下降,需要对两棵超级树包含的所有小波树按能量进行排序,按奇偶序列划分小波树到两棵超级树,使得两棵超级树的能量相近。此算法需要保存超级树的组成信息作为嵌入和提取的密钥。文献[4,5]等提出的算法也是在跨子带的树结构下,通过改变小波系数的幅值来嵌入水印信息。文献[7]对中频子带LH3的系数进行分组,通过对组中的最大系数(相对重要的小波系数)采用不同的量化方法来嵌入水印信息,虽然取得了一定的效果,但由于块的划分基于空间顺序,很容易通过对局部最大系数值的修改进行攻击;且在嵌入水印bit'0'时,部分最大系数值量化幅度较大,使得水印的安全性和嵌入后图像的视觉效果均不理想。

本文对小波系数的特性与SDQ算法进行了分析,提出了一种充分利用中频子带中重要系数相对关系的、安全、鲁棒的盲水印算法。对比文献[7]提出的小波系数显著性差异量化(SDQ)嵌入算法,改进的算法伪随机选取两块数据组成一组,具有更高的安全性。改进的算法尊重每组系数中最大的两个系数之间的相对大小关系,为了强化相对大小关系,小幅度量化重要系数,而不是如文献[7]那样为了嵌入某些水印信息,通过大幅度修改重要系数来改变重要系数的大小关系。嵌入策略的修改不仅使水印图像的质量下降很小,而且对jpeg压缩、多种滤波、缩放、裁剪和轻微角度的旋转攻击均有更好的抵抗能力。

## 2 小波系数的特性与SDQ算法

小波变换不同于其它变换,是因为其具有独特的时频局

到稿日期:2009-12-17 返修日期:2010-03-05 本文受国家自然科学基金(No. 60803136),广州市科技计划(No. 2009J1-C541-2)资助。
胡 青(1975-),女,博士生,讲师,主要研究方向为信息安全、图像数字水印,E-mail:huqing299@sohu.com;龙东阳(1958-),男,教授,博士生导师,主要研究方向为信息安全、编码理论;卢 伟(1979-),男,博士,讲师,主要研究方向为信息隐藏、图像数字水印。

部化特征，每个小波系数代表确定频率范围和局部空间的信息。在这个意义上说，每个小波系数都是图像的特征值。小波系数的幅值越大，说明这样的一个时频特征在对应的图像中非常显著，它所包含的图像的能量也就越大，相对于整个小波系数集它的重要性也越大。我们把它称为重要系数[7]。Kutter 等[8]提出了第二代水印的概念。第二代水印方案的主要思想就是根据数据的重要特征嵌入水印信息，把水印信息和图像特征紧紧地联系在一起，以期获得更好的隐蔽性和鲁棒性。因此，本文提出的水印算法设计思路是围绕着如何有效地利用这些重要系数。

对于鲁棒水印算法，透明性和鲁棒性是两个最根本的要求。从统计属性上来看，低频子带到高频子带具有父子关系的小波系数的幅值衰减。低频子带中小波系数幅值非常大，聚集了图像的大部分能量，对低频系数的轻微修改可能会造成图像明显失真。而高频子带中的小波系数代表了图像的细节信息，对低通滤波、加噪等处理非常敏感。因此，我们应该选中频子带中最重要的系数来嵌入水印信息。SDQ 算法选取在 LH3 子带中嵌入水印信息，因为相对于其它子带来说，这个子带中包含较多的重要系数，是除低频子带外最重要的子带。在这个子带中嵌入水印信息，能较好地平衡水印信息的透明性和鲁棒性。文献[7]指出，虽然图像经过各种攻击以后，小波系数的值会产生变化，但小波系数幅值之间的大小关系保持一定的稳定性。正是基于这一事实，SDQ 算法通过差异量化局部最大值来嵌入水印信息。首先对原始图像进行 3 层小波变换（如图 1 所示），然后对变换后的中频子带 LH3（或 HL3）的系数进行分块（分组），每块嵌入 1bit 水印信息。块的大小可根据需要嵌入的水印信息量和希望的嵌入强度等综合决定。若嵌入信息为'0'，则量化最大系数值使之与次大系数相等来嵌入；若嵌入信息为'1'，则按需要量化最大系数的值使之与次大系数的差值大于某一阈值。同理，在提取水印时，根据每块系数中最大系数和次大系数的差值大小提取水印信息。

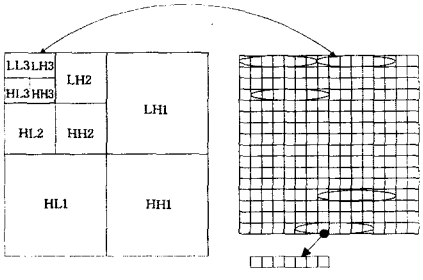
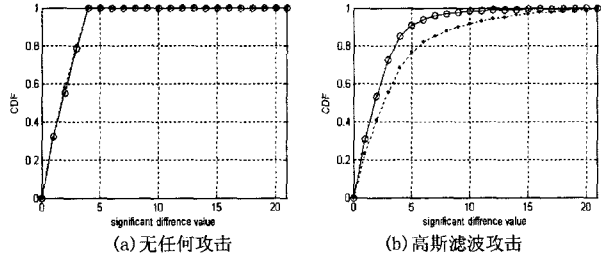



图 1　SDQ 算法 LH3 子带系数分组方案

SDQ 算法为了在块内嵌入 1bit 水印信息差异量化块中最大系数的幅值，特别当嵌入信息为'0'时，量化最大值的大小使之等于次大值的大小。若次大值远远小于最大值，那么最大值这个代表某一时频局部化特征的量就会改变得过多，虽然峰值信噪比这一客观评价指标的值仍然可以保持在 45dB 左右的高水平，但嵌入水印后图像局部视觉上产生了较大的失真。不仅如此，通过对大量图像实验数据的统计分析，发现 SDQ 算法中大幅度量化最大系数造成的最大系数与次大系数近似相等的特征对各种图像处理和攻击的稳定性较差。针对 10 幅 512×512 的标准测试图像[9]（lena，baboon，f16，couple 等），每幅图像分别按 SDQ 算法抽取 100 组嵌入'0'信息的块和 100 组最大系数与次大系数值较接近的小波系数数据块，通过统一的量化策略（块内的最大系数值量化为次大系数值）进行量化，而后对各种攻击下最大系数和次大系数的差值进行了统计分析。我们用带黑点的虚线表示按 SDQ 算法嵌入'0'后对应的最大系数和次大系数差值的累计分布函数（CDF）曲线，用带空心圆圈的实线表示原最大值与次大值较接近的情况下，最大系数值量化等于次大系数之后，最大系数和次大系数差值的累计分布函数（CDF）曲线。图 2（a）表明在无任何攻击的情况下，依 SDQ 算法量化的最大系数和次大系数值的差异 CDF 曲线与原始最大系数与次大系数较接近情况下量化的差异 CDF 曲线基本重合。图 2（b）表明在高斯滤波攻击下，按 SDQ 算法量化得到的重要系数差值近似相等的特征的稳定性较差。对于其它的图像处理（中值滤波、加噪、旋转、压缩等）也有相似的结果，即实线在虚线之上。也就是说，相对大幅度量化获得的重要系数近似相等的相对关系，在原有的两个最大系数相差不大的情况下，通过小幅度量化获得的近似相等的相对关系具有更强的稳定性。所以无视原始图像小波系数值的分布，为了嵌入水印信息而强行大幅度地对重要系数进行修改，显然是不合适的。




（a）无任何攻击　　（b）高斯滤波攻击

图 2　本文的量化方案与 SDQ 效果对比

另外，SDQ 算法的安全性由种子（密钥）控制下的伪随机交换打乱块的次序来保证。虽然攻击者不知道密钥就无法正确地组织提取的水印信息比特，但由于块的划分基于小波系数位置上的相邻关系，即使不需要知道密钥，攻击者仍然可以非常容易地找到局部最大值和次大值，通过对它们的修改来改变差值，从而破坏掉水印信息。

## 3　改进的嵌入和提取水印算法

上节的实验数据表明大幅度地修改重要系数，不仅会造成图像质量的下降，而且会使得修改后的重要系数相对大小关系稳定性下降。因此我们的嵌入算法没有强制性地改变重要小波系数间原有的相对关系，而是通过修改重要系数的值来加强这种相对关系，确保这种相对关系对各种攻击具有较强的稳定性。为了加强算法的安全性，防止水印信息被擦除，我们的算法把 LH3 子带中属于同一父系数的 4 个系数自然地组成一块（块的大小可根据水印信息的大小、嵌入强度等因素确定），在密钥 key1 的控制下，伪随机地选择两块共 8 个小波系数组成一组数据，每组数据嵌入 1bit 水印信息。若原始图像大小为 512×512，则 LH3 子带中共有 64×64 个小波系数，可伪随机分为 512 组，每组嵌入 1bit 水印信息，即最多可在 LH3 子带中嵌入 512bit 水印信息。与 SDQ 算法相比，我们的分组方法不是简单地根据自然的位置分布来分组，而是在 key1 的控制下选择两块数据组成一组数据，如图 3 所示。这样攻击者没有密钥 key1 就无法猜测哪两块数据组成一组，

既不能提取水印信息，也无法通过修改组内最大系数的值来破坏水印。

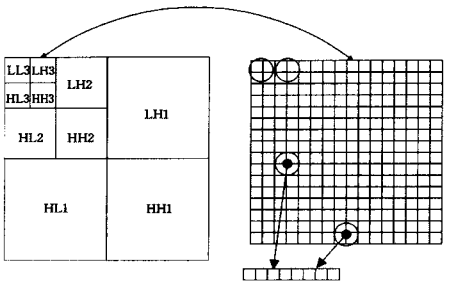



图 3　本文的 LH3 子带系数分组方案

具体的嵌入算法步骤如下。

S1：原始图像分解。对原始图像做 3 级 haar 小波分解，提取出中低频子带 LH3(或 HL3)的小波系数，LH3 子带中属于同一父系数的 4 个系数作为一块数据。

S2：在密钥 key1 的控制下，伪随机地挑选两块数据(共 8 个小波系数)组合为一组数据，依次对 LH3 子带中的小波系数进行分组。

S3：根据需嵌入水印信息的大小，循环处理第 $i$ 组小波系数，嵌入水印信号中第 $i$ 位的信息。max1($i$)，max2($i$)表示组内的最大系数值和次大系数值。watermark($i$)表示需要嵌入水印的第 $i$ 位信息。$T$ 为正数，是水印信号嵌入时设定的阈值。

1)计算第 $i$ 组系数中最大的两个系数之差 $disp$：

$disp$=max1($i$)−max2($i$)；

a)若 $disp>T$，则 $f(i)=1$，表示两个重要系数的能量具有显著的差异；如果 $disp<2T$，则量化组内的最大系数 max1($i$)=max1($i$)+$T$，加强这种差异；

b)若 $disp<T$，则 $f(i)=0$，表示这两个重要系数能量接近，则量化组内的最大系数 max1($i$)=max2($i$)，使两个最大系数能量更接近；

2)根据这组系数的特征 $f(i)$的值和嵌入的水印信息，计算密钥 key2 的对应比特位：

key2($i$)=$f(i)$⊕ watermark($i$)；

S4：保存 key2 作为提取水印所需的第二个密钥，逆变换重构图像。

算法通过 $T$ 值来判定两个重要系数的大小是否存在差异，决定特征值为 1 还是 0，密钥 key2 的第 $i$ 位信息由 $f$(i)⊕ watermark($i$)得到；⊕表示按位的异或运算。若 $T$ 值过大，则大部分分组特征值为 0，使得对应的 key2($i$)等于 watermark($i$)，即密钥 key2 与水印相关系数值太大。$T$ 过小，会降低水印的抗攻击能力。实验中我们取小波图像所有分组中两个最大系数差值的中值作为阈值 $T$，既保证了鲁棒性，也使得密钥 key2 与水印的相关系数 $NC$ 趋于 0。

水印的提取算法与嵌入算法相似，过程非常简单。本算法属于盲水印，提取过程无需原始图像，但需要使用密钥 key1 对 3 级小波分解后形成的 LH3 子带的小波系数进行同样的伪随机分组。在密钥 key2 的控制下比较同一分组中两个最大系数差来提取嵌入在这一分组中的 1bit 水印信息。$T$ 取嵌入水印图像所有分组中两个最大系数差值的中值。对嵌入在第 $i$ 个分组的第 $i$ 位的水印信息提取步骤如下：

1)计算两个最大系数的差值，$disp$=max1($i$)−max2($i$)；

2)比较这两个差值，确定这组系数的特征，若 $disp>T$，则 $f(i)=1$；否则 $f(i)=0$；

3)提取嵌入这组系数的 1bit 水印信息，watermark($i$)=$f$($i$)⊕ key2($i$)。

我们注意到，虽然提取水印时需要多传递一个密钥 key2，但这个密钥使得水印嵌入时在阈值 $T$ 的控制下，可以通过小幅度的量化来保证水印的嵌入强度。本文的算法保持同组重要小波系数之间的相对关系，而不是为嵌入水印信息通过大幅度量化来建立重要系数之间的相对关系[7]。因此本文提出的水印算法的透明性和鲁棒性均有显著的提高。由于每组的两块小波系数位置伪随机分布，不知道密钥 key1 就很难破坏水印信息。水印嵌入算法根据组内两个最大值的差值特征，通过小幅度的量化来强化特征，密钥 key2 是在水印的嵌入过程中逐步生成的，由图像系数特征和水印信息同时决定。即使获得 key1，不知道密钥 key2 也无法正确提取水印信息。水印算法的安全性通过这两个密钥得到了很好的保障。

## 4　实验结果

我们使用峰值信噪比($PSNR$)来客观估计图像的质量，$PSNR$ 定义为：

$$PSNR=10\times\log_{10}\frac{255\times255}{\frac{1}{H\times W}\sum_{x=0}^{H-1}\sum_{y=0}^{W-1}[f(x,y)-g(x,y)]^2}\text{dB} \tag{1}$$

式中，$H$ 和 $W$ 表示图像的长度和宽度，$f(x,y)$和 $g(x,y)$分别表示原图像和受攻击图像在$(x,y)$位置的灰度值。提取出水印信息后，用原始水印和提取水印的归一化相关系数($NC$)来客观判断水印是否存在。$NC$ 定义如下：

$$NC=\frac{1}{w_h\times w_w}\sum_{i=0}^{w_h-1}\sum_{j=0}^{w_w-1}w(i,j)\times w'(i,j) \tag{2}$$

式中，$w_h$，$w_w$ 分别表示水印图像的长度和宽度，$w(i,j)$和 $w'(i,j)$代表原始水印图像和提取的水印图像在$(i,j)$位置的值。在式(2)中，若水印比特为'1'，则 $w(i,j)$值为 1；否则为−1。$w'(i,j)$的值以同样的方法设定。

下面利用 stirmark，AdobePhotoshop 和 matlab 软件工具来模拟一些常规的图像处理和攻击。通过比较不同情况下提取的水印信号与嵌入信号的相关系数来分析算法的性能。

本文特别以 512×512 的灰度图像 lena 为例，对文献[7]算法和改进算法的实验结果进行比较。嵌入 32×16 的二值图像作为水印信号。图 4(a)为原始图像；图 4(b)为嵌入水印图像；图 4(c)为本文算法嵌入水印后的图像，峰值信噪比为 57.29；图 4(d)为文献[7]算法嵌入水印后的图像，峰值信噪比为 44.25。

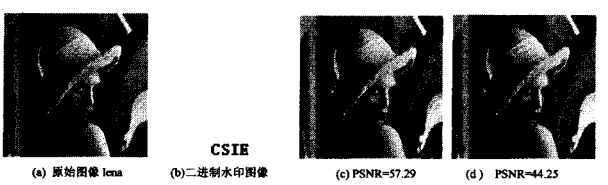



图 4　嵌入水印图像质量对比

(1)抗 JPEG 攻击

JPEG 是网络和数码相机中最常用的一种图像格式，质

量因子的值为0～100，对于JPEG的攻击算法应该具有较强的鲁棒性，试验结果如表1所列。可见本文提出的算法与文献[7]提出的算法相比，嵌入水印后的图像具有更好的图像质量，而且在质量因子低于30的JPEG压缩下还能很好地提取出水印信息。

表1　不同质量因子下水印检测结果对比

| NC\QF | 10 | 15 | 20 | 25 | 30 | 40 | 50 |
|---|---|---|---|---|---|---|---|
| 算法[7] | 0.41 | 0.57 | 0.68 | 0.80 | 0.87 | 0.95 | 0.98 |
| 本算法 | 0.78 | 0.81 | 0.83 | 0.84 | 0.93 | 0.99 | 1 |
| 提取水印 | CSIE | CSIE | CSIE | CSIE | CSIE | CSIE | CSIE |

(2)非几何攻击

对嵌入水印后的图像进行各种滤波处理和噪声等攻击，试验表明本文提出的算法具有很强的抵抗干扰的能力。结果如表2所列，表中*PSNR*代表的是嵌入水印信息的图像和经过滤波、加噪处理后图像的峰值信噪比。

表2　滤波、加噪等攻击下水印检测结果对比

| NC\攻击 | 中值滤波 | | | 均值滤波 | | |
|---|---|---|---|---|---|---|
| | 3×3 | 5×5 | 7×7 | 3×3 | 5×5 | 6×6 |
| 算法[7] | 0.88 | 0.74 | 0.57 | 0.91 | 0.72 | 0.53 |
| 本算法 | 0.96 | 0.83 | 0.71 | 0.92 | 0.79 | 0.68 |
| 提取水印 | CSIE | CSIE | CSIE | CSIE | CSIE | CSIE |

| NC\攻击 | 高斯滤波 | 锐化 | 直方图均衡 | 高斯噪声 | | |
|---|---|---|---|---|---|---|
| PSNR | 40.19 | 21.75 | 18.80 | 29.91 | 23.90 | 20.37 |
| 算法[7] | 0.86 | 0.99 | 0.77 | 0.91 | 0.54 | 0.50 |
| 本算法 | 0.99 | 0.99 | 0.88 | 0.95 | 0.63 | 0.53 |
| 提取水印 | CSIE | CSIE | CSIE | CSIE | CSIE | CSIE |

(3)几何攻击

本算法是基于小波变换的盲水印算法，其抵抗几何攻击的能力虽然比文献[7]算法有一定的提高，但与文献[7]算法一样，提取水印之前还需要进行恢复同步的处理。对于缩放攻击，我们利用Adobe Photoshop软件先缩小图像为256×256，然后放大为512×512大小。同样地，对于从裁剪后的图像中提取水印前我们必须对裁剪位置补上0或其它值，以保持同步性。小尺度旋转后，我们只须对图像的边缘进行必要的裁剪，使其仍然为512×512大小的图像。对于大尺度的旋转，我们则必须能较精确地估计出旋转的尺度，通过逆旋转来保证同步。虽然对于单一的几何攻击算法具有一定的鲁棒性，但如果对嵌入水印图像进行复杂的几何攻击，那么提取水印难度会加大。表3列出了几何攻击下的水印检测结果。

表3　几何攻击下水印检测结果对比

| 攻击\NC | 缩放1/2 | 裁剪1/4 | 小角度旋转(°) | | | | |
|---|---|---|---|---|---|---|---|
| | | | 0.5 | 0.3 | 0.25 | −0.25 | −0.3 |
| 算法[7] | 0.86 | 0.70 | - | 0.57 | 0.67 | 0.67 | 0.57 |
| 本算法 | 0.95 | 0.77 | 0.69 | 0.76 | 0.78 | 0.83 | 0.79 |
| 提取水印 | CSIE | CSIE | CSIE | CSIE | CSIE | CSIE | CSIE |

我们还对多幅图像[9]进行了实验。虽然相比文献[7]算法在进行水印嵌入和提取时需要一个与水印信息同样大小的密钥key2，但嵌入水印的图像质量和抵抗攻击的能力均有显著提高。如图5所示，水印图像(a)Peppers，(b)Airplane，(c)Bridge，(d)Couple保持了较高的图像质量，表4列出了部分试验结果。

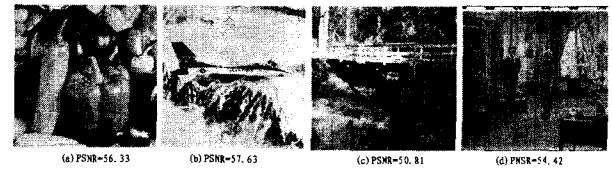



图5　多幅图像嵌入水印后的*PSNR*

表4　多幅图像各种攻击下的水印检测结果

| 攻击\NC | | Peppers | Airplane | Bridge | Couple |
|---|---|---|---|---|---|
| JPEG压缩(QF) | 40 | 0.98 | 0.97 | 1 | 0.99 |
| | 30 | 0.90 | 0.93 | 1 | 0.96 |
| | 20 | 0.86 | 0.88 | 0.98 | 0.89 |
| | 10 | 0.72 | 0.79 | 0.83 | 0.71 |
| 中值滤波 | 3×3 | 0.97 | 0.96 | 0.93 | 0.92 |
| | 5×5 | 0.86 | 0.78 | 0.72 | 0.77 |
| | 7×7 | 0.76 | 0.66 | 0.51 | 0.63 |
| 高斯滤波 | | 0.99 | 1 | 0.99 | 0.98 |
| 高斯噪声(var) | 1 | 0.95 | 0.96 | 1 | 0.97 |
| | 2 | 0.77 | 0.73 | 0.96 | 0.78 |
| | 3 | 0.50 | 0.58 | 0.80 | 0.59 |
| 直方图均衡 | | 0.88 | 0.50 | 0.87 | 0.73 |
| 缩放(50%) | | 0.95 | 0.96 | 0.93 | 0.98 |
| 旋转 | 0.3 | 0.74 | 0.72 | 0.61 | 0.64 |
| | 0.25 | 0.77 | 0.77 | 0.70 | 0.71 |
| | −0.25 | 0.78 | 0.73 | 0.66 | 0.74 |

**结束语**　本文提出的盲水印算法充分利用小波变换后中频重要系数值的相对关系对于常规的攻击具有很强的抵抗能力这一事实，通过密钥尽可能少地修改重要系数值，不仅大幅提高了嵌入水印图像的质量，而且没有密钥信息，无法提取和破坏水印。通过对水印信息嵌入前的纠错编码，或利用其他(HL3，HH3等)子带重复嵌入等方法可进一步提高算法的性能。由于算法基于小波变换，小波域并非几何不变域，因此抵抗复杂几何攻击的能力还有待提高。下一步我们将思考如何结合其他方法进一步增强算法抵抗几何攻击的能力。

## 参考文献


[1] Hsu Chiou Ting, Wu Jaling. Hidden digital watermarks in images[J]. IEEE Transactions on Image Processing, 1999, 8(1): 58-68

[2] Wang Shih-hao, Lin Yuan-pei. Wavelet tree quantization for copyright protection watermarking[J]. IEEE Transactions on Image Processing, 2004, 13(2): 154-165

[3] Das T K, Maitra S. Analysis of the "Wavelet Tree Quantization" watermarking strategy and a modified robust scheme[J]. Multimedia Systems, 2006, 12: 151-163

[4] Tsai Min-jen, Chen Bai-jiun. Tree Energy Differentiation (TED) based wavelet watermarking for digital images[C]// ICIP 2008. 2008: 445-448

[5] Lin Wei-hung, Wang Yuh-rau, Hog Shi-jinnrn. A wavelet-tree-based watermarking method using distance vector of binary cluster[J]. Expert Systems with Applications, 2009, 36: 9869-9878

[6] Cox I J, Kilian J, Leighton F T, et al. Secure spread spectrum watermarking for multimedia[J]. IEEE Transactions on Image Processing, 1997, 6(12): 1673-1687

[7] Lin W H, Horng S J, Kao T W, et al. An Efficient Watermarking Method Based on Significant Difference of Wavelet Coefficient Quantization[J]. IEEE Transactions on Multimedia, 2008, 10(5): 746-757

[8] Kutter M, Jees B, Ebrahimit K. Towards second generation watermarking scheme[A]// Proc. of ICIP'99[C]. Kobe, Japan: IEEE, 2002, 1: 320-323