# TURBO 码在数字水印鲁棒算法中的应用*)

胡艳维[1] 秦 拯[1,2]

(湖南大学软件学院 长沙 410082)[1] (东莞理工学院软件学院 东莞 523808)[2]

**摘 要** Turbo 码在低信噪比时具有优异的纠错性能,已经成为通信研究的前沿。一个典型的数字水印系统从原理上可等效为一个通信系统。针对在图像中嵌入大容量水印难度大的问题,提出把 Turbo 码应用到数字水印系统中,用来提高水印系统的鲁棒性,在算法中采用标志位信息的增强方式,提取秘密信息;采用 Turbo 码译码方法,以恢复原始的水印。实验结果表明,改进后的方案明显优于原方案,特别是在高斯噪声影响下。

**关键词** Turbo 码,水印嵌入,水印信息提取

## TURBO Codes in Digital Watermark Robust Algorithm Application

HU Yan-Wei[1] QIN Zheng[1,2]

(Software College of Hunan University, Changsha 410082)[1]

(Software College of Dongguan University of Technology, Dongguan 523808)[2]

**Abstract** The low signal-to-noise ratio Turbo codes have the outstanding error correction performance, and already became the correspondence research front. A typical digital watermark system by theory may be equivalent to a communications system. In view of inserts the large capacity watermark difficulty major problem in the image, proposed applies the Turbo codes in the digital watermark system, uses for to enhance the watermark system robustness, uses the flag bit information in the algorithm the enhancement way, withdraws the secret information; uses the Turbo codes decoding method, restores the primitive watermark. The experimental result indicated that, specially under the Gauss noise influence, after the improvement plan obviously surpasses the original plan.

**Keywords** Turbo code, Watermark inserting, Watermark information extraction

Turbo 码是信息论之父克劳德·香农发现的。开始,Turbo 码主要是用于卫星串路。现在这个技术正在视频信号、图形图像信号的通信、数字音频、视频广播、增强型无线互联网等领域发挥越来越大的作用。Turbo 码的这种巨大前景,使其成为通信研究的前沿。Turbo 码能设计出非常接近信道容量(即在一定发射功率电平下信道可传输的每秒比特数值的绝对最大容量)的系统。

在典型的通信系统中,因为 Turbo 码在低信噪比时具有优异的纠错性能而备受关注。而一个典型的数字水印系统从原理上可等效为一个通信系统[1],因此有人提出把 Turbo 码应用到数字水印系统中,用来提高水印系统的鲁棒性。

## 1 改进前的水印信息提取方案

Lee Jun 等人在 2001 年的国际图像处理会议(ICIP)上提出了一种利用 Turbo 码的水印信息提取方案[2]。在他们提出的方案中,有意义的水印 LOGO 并没有像通常的方法一样把 LOGO 嵌入到图像的 DCT 域,而是首先在图像的 DCT 域提取一个二进制的标志位信息序列,然后把提取的标志位序列与经过 Turbo 编码的 LOGO 序列二值相加,得到一个秘密信息序列,也就是密钥。这个密钥将作为水印 LOGO 提取的唯一通道,从而能达到保护版权的目的。

### 1.1 水印嵌入

与一般的水印嵌入方案不同的是,在文[3]提出的水印方案中,选取的有意义的水印 LOGO 并没有直接嵌入到载体图像中,而是首先把 LOGO 经过 Turbo 码编码,然后再与从图像的 DCT 域提取的标志位信息进行二值相加,生成只有嵌入者知道的秘密信息(SI),为了表达的方便,这里仍然把 SI 的生成过程称为水印的嵌入过程。嵌入原理框图如图 1 所示。

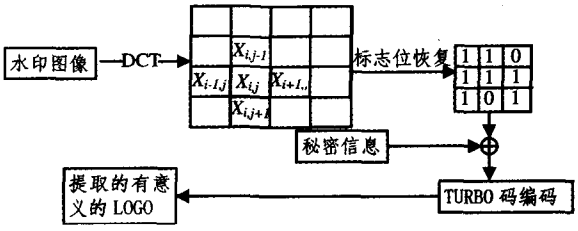



图 1 水印嵌入原理框图

这里首先要说明的是水印信息,即有意义的 LOGO,LOGO 的选择必须具有受保护的意义,如:公司的注册商标等可以作为有意义的 LOGO,在实验中,选择较有意义的 LOGO。这里讨论的 LOGO 为一幅二值图像,在进行 Turbo 编码之前,必须把 LOGO 转变为二进制序列的形式,即 $\overline{d}=(d_{1N},\cdots,d_N)$。其中,$d_1\in\{0,1\}$,$N$ 为 LOGO 图像的大小。这样,Turbo 码编码器的输出二进制序列为:$\overline{b}=(b_{1M},\cdots,b_M)$,其中 $b_i\in\{0,1\}$,$M$ 为编码后二进制序列的大小。

在提取标志位信息时,首先把原始图像变换到 DCT 域,然后随机选择一个 DCT 系数 $x_{i,j}$ 作为中心参考系数(这里把 $x_{i,j}$ 作为中心)。记录下中心参考系数的位置,并求出其四邻域系数的平均值:

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

同时,比较中心参考系数与平均值 $m_{i,j}$ 的大小,生成标志位信息 $f_k$。

*)资助项目:国家自然科学基金项目(No. 60273070),湖南省科技计划项目(No. 2006FJ4110),东莞市科研发展基金项目(No. 2006D46,2005D049)。**胡艳维** 硕士研究生,CCF 会员,主要研究方向为信息安全、数字水印;**秦 拯** 博士,CCF 会员,教授。

$$f_k=\begin{cases}1 & \text{当 } x_{i,j}>m_{i,j}\\ 0 & x_{i,j}\leqslant m_{i,j}\end{cases} \tag{2}$$

其中 $1\leqslant k\leqslant M$，也就是说，标志位序列的大小与编码后的LOGO序列大小相同。获得标志位信息的同时，把中心参考系数乘以一个加权因子来加强中心参考系数与其四邻域平均值 $m_{i,j}$ 之间的关系，达到增强标志位信息的鲁棒性的目的。这种鲁棒性的增强将在LOGO的提取过程中得到体现。

$$x'_{i,j}=\begin{cases}x_{i,j}+\alpha\cdot x_{i,j}=(1+\alpha)\cdot x_{i,j}, & \text{当 } x_{i,j}\leqslant m_{i,j}\\ x_{i,j}+\alpha\cdot x_{i,j}=(1-\alpha)\cdot x_{i,j}, & \text{当 } x_{i,j}>m_{i,j}\end{cases} \tag{3}$$

这里，仍然把参数 $\alpha$ 称为嵌入强度因子，$\alpha$ 的选择需在LOGO信息的鲁棒性与被修改图像的质量之间进行选择。当全部标志位信息提取出来后，把修改后的DCT系数矩阵进行反DCT变换，获得增强了标志位信息的图像，这里也把它称为水印图像。然后把从图像提取的标志位信息序列与Turbo码编码后的水印序列二值相加得到秘密信息，由作品所有者保存。

### 1.2 水印检测

检测水印时，即LOGO的提取过程，不需要原始图像与原始水印，这也是一种全盲的水印检测算法，水印的检测过程如图2所示。

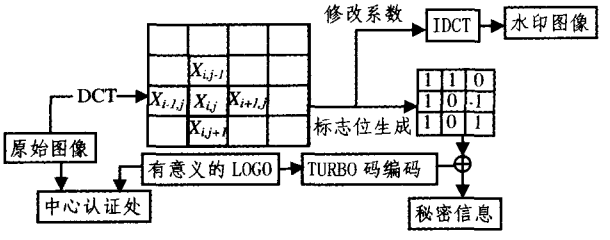



图2 LOGO提取原理框图

检查过程比较简单，首先把可能遭受攻击的水印图像变换到DCT域，在系数被修改过的位置提取出可能被“污染”过的标志位信息：

$$f'_k=\begin{cases}1 & \text{当 } x''_{i,j}>m'_{i,j}\\ 0 & \text{当 } x''_{i,j}<m'_{i,j}\end{cases} \tag{4}$$

其中，$x''_{i,j}$ 是可能遭受攻击的水印图像的DCT系数。然后把可能受损的标志位信息与保存的秘密信息二值相加。这样，得到的是含有错误的经过编码保护的LOGO二进制序列，再经过Turbo码纠错译码后，得到错误矫正后的LOGO。

## 2 改进的水印信息提取方案

### 2.1 水印嵌入方案的改进

本论文在改进前的方案中，中心参考点是随机选择的，也就是说，水印的嵌入位置是随机选择的，随机选择的结果是可能包含一些低频分量和一些高频分量，而高频分量承载的水印信号很容易被有损的数字化处理所破坏，低频分量承载的水印信号容易降低水印的不可见性，即降低水印图像的质量。当要求嵌入的水印容量较大时，这种情况就会变得很明显。

除此之外，随机选择中心参考点的不足之处在于：当嵌入的水印数据量较大时，相邻两点同时成为中心参考点的可能性很大，这样会引出一个问题：假设某个DCT系数被确定为是中心参考系数，记为 $x_{i,j}$，如果 $x_{i,j}$ 比其四邻域平均值大的话，那么就需要修改 $x_{i,j}$ 的值，即：

$$x'_{i,j}=x_{i,j}+\alpha\cdot x_{i,j} \tag{5}$$

同时，如果 $x'_{i,j}$ 成为另一个中心参考点的四邻域系数中的某一个系数，假设这个中心参考系数为 $x_{1+i,j}$，同时假设这个系数大于其四邻域的平均值，那么这个系数被修改为：

$$x'_{i+1,j}=x_{i,j}+\alpha\cdot x_{i+1,j} \tag{6}$$

这样，就相当于增大了 $x'_{i,j}$ 的四邻域的平均值 $m'_{i,j}$，也就说在水印嵌入过程中就降低了水印的鲁棒性。

再来看式(3)的标志位信息的增强方式。当中心参考系数 $x_i$ 小于零时，如果按照式(3)的方式修改，假设修改之前 $x_{i,j}$ 的值大于其四邻域的平均值的话，那么修改后的 $x_{i,j}$ 的值将更小，经过修改后的系数的值将有可能小于其四邻域的平均值。也就是说，当嵌入数据量较大的时候，这种修改方式很可能直接就引入了错误，即直接降低了水印信号的鲁棒性。因此，可以得出这样的结论：文[2]中的好的鲁棒性只是在嵌入容量较低的情况下获得的，不具有普遍性。面对这些不足之处，对水印的嵌入方案做了一定的改进。接下来，将详细展开改进的修改方案。

首先，为了避免随机选择中心参考系数可能带来的修改图像高频和低频的DCT系数的问题，把图像的DCT系数从左上角开始，按照之字行顺序进行重新排序，经过这样重新排序获得的系数序列的频率恰好按照从低到高的顺序排列。这样，就可以把这个序列的中间的系数看成是图像的中频分量，如果在这个区间进行系数修改的话，就可以避免高频分量与低频分量的影响。

其次，为了避免中心参考点的四邻域系数被修改的可能性，在修改系数的过程中，并不把图像所有的DCT系数进行重新排序输出，而是按照上述的顺序进行系数的修改。首先假设其中频起始位置的系数为中心参考系数，把这个位置标记为1，然后按照之字形顺序进入下一个位置，判断其四邻域上有没有标记为1的位置，如果有的话，按照之字形顺序进入下一个系数。如果其四邻域上没有标记为1的位置，那么就在这个位置上修改中心系数，同时，记住这个位置的坐标，并且把这个位置标记为1。按照这种算法直到嵌入所有的编码比特信息。其具体的修改过程如图3所示。

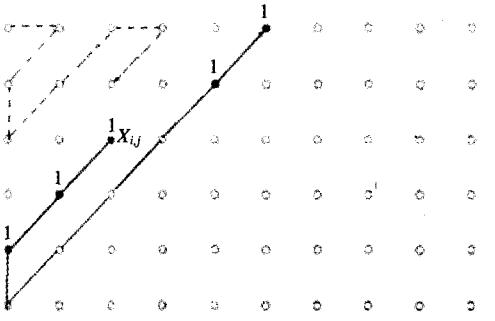



图3 改进的系数修改方案

其中，虚线表示DCT系数的排序方向，实线表示系数的修改方向，两者之间方向相同，不同的是起始位置不一样，前者的起始位置为直流分量，后者的起始位置是事先约定的中频起始位置。实心的坐标点表示被修改过的系数，空心的则是没有修改过的系数，从上图中可以看出：以这种方式最多只有一半的DCT系数能被修改。

为了避免式(3)这种修改方式所碰到的问题，采用了下面的修改方式来加强标志位信息。这种标志位信息的加强仍然体现在标志位信息提取时。

$$x'_{i,j}=\begin{cases}x_{i,j}+alpha & \text{当 } x_{i,j}\leqslant m_{i,j}\\ x_{i,j}+alpha & \text{当 } x_{i,j}>m_{i,j}\end{cases} \quad (7)$$

这里，把参数 alpha 称为嵌入强度，在选取 alpha 的值时，需要同时考虑修改后的标志位信息的鲁棒性和发布的水印图像的质量。一般根据经验值得出。alpha 过小，那么标志位信息很容易被破坏，从而使 LOGO 的恢复变得困难；如果 alpha 过大的话，那么修改后的图像的质量会变坏，损坏水印的不可见性，影响图像的视觉效果。

改进方案的秘密信息的生成过程如下：

1. 在某个中心认证处注册原始图像以及有意义的原始水印 LOGO(如公司的商标等)。

2. 把原始图像变换到 DCT 域。

3. 从图像 DCT 系数的直流分量开始按之字形扫描至事先确定的中频起始位置 $x_{i,j}$，如图 3 所示，并把该位置的系数作为中心参考系数，在本文中，中频起始位置为扫描顺序上的第 6001 个系数的位置。

4. 对于 DCT 中频域中的中心参考系数 $x_{i,j}$，求出其四邻域的平均值 $m_{i,j}$，根据(3-1)进行计算，如果坐标发生溢出，则补 0 后再求平均值。

5. 根据 $x_{i,j}$，与 $m_{i,j}$ 之间的相对关系，按照式(7)对 $x_{i,j}$ 做出修改，目的是加强标志位信息的鲁棒性，使得在提取标志位信息时，这种中心参考系数与其四邻域的平均值之间的相互关系即使在遭受某种攻击之后仍然能保持不变。在修改中心参考系数的同时，可以根据式(2)提取出标志位信息。

6. 扫描下一个 DCT 系数，判断该系数的四邻域系数中是否有被修改过的系数。如果有，则扫描下一个系数；否则，将该系数设为中心参考系数，重复上述步骤 4 和 5 直到提取的标志位信息序列与编码后的水印 LOGO 序列大小相同。

7. 经过 Turbo 码编码的水印 LOGO 序列与标志位信息序列二值加后便得到了用于提取 LOGO 的秘密信息(SI)。

8. 经过 DCT 反变换获得加强了标志位信息的图像。

### 2.2 水印 LOGO 提取

水印 LOGO 的提取过程如图 2 所示，也就是说采用了原有的水印 LOGO 的提取方案。

水印 LOGO 的提取步骤如下：

1、将待检验的水印图像变换到 DCT 域。

2、按照系数修改方案找出所有被修改过的位置，求出可能被“污染”的中心参考系数的四邻域的平均值：

$$m'_{i,j}=(x''_{i-1,j}+x''_{i+1,j}+x''_{i,j-1}+x''_{i,j+1})/4 \quad (8)$$

按照式(4)比较四邻域平均值 $m'_{i,j}$ 与中心参考系数 $x''_{i,j}$ 的大小关系，重新生成可能被“污染”的标志位信息 $f'_k$。

3、把可能被“污染”的标志位序列 $f'$ 与保存的秘密信息进行二值相加得到可能含有错误的水印 LOGO 序列。

4、将第三步得到的水印 LOGO 序列进行 Turbo 码译码，力求恢复为原始的水印 LOGO。

## 3 实验结果

在实验中，使用了与原文献相同的原始图像，图像大小为 256×256，如图 4(a)所示。原始水印 LOGO 为 60×40 的有意义的二值图像，如图 4(c)所示。取值远远大于原有方案的目的是想证明当嵌入容量较大时，原有的方案的修改方法并不稳定。Turbo 码编码单元均为(7,5)的递归系统卷积码，交织器是 60×40 的伪随机交织器，编码效率为 1/3，Turbo 译码算法采用了低复杂度的 MAX-LOG-MAP 算法，仿真结果如图 4 所示。译码迭代次数为 6 次。预定义的中频系数起始位置为 6001，门限阈值为 15，嵌入水印的图像如图 4(b)所示。


(a)原始图像 256×256　(b)加强了标志位的图像　(c)原始 LOGO

图 4　嵌入水印的图像

对水印图像做了两类攻击：标准攻击和非标准攻击。标准攻击是指在标准攻击软件 Stirmark3.1[4] 中所包含的基本攻击，其中包括图像的数字化处理操作和基本的几何攻击。Stirmark 是由剑桥大学专门开发的用于测试一个水印系统的鲁棒性的标准软件，3.1 是其推出的最新版本。非标准攻击是指在标准攻击中所不包含的攻击，非标准攻击后的水印图像如图 5 所示，其中高斯噪声攻击的均值为 0，方差为 0.01；维纳滤波窗大小为 3×3。每个受攻击后的图像左下角为改进前方案提取的水印 LOGO，右下角为改进后方案提取的水印 LOGO，改进前和改进后方案的水印检测错误率的比较见表 1 和表 2，这里水印检测错误率是指提取出来的水印相对于原始水印来说有多少是错误的。

表 1　非标准攻击的检测结果对比

| 攻击 | 改进后方案<br>改进前方案 | 检测错误率<br>检测错误率 |
|---|---|---|
| 标准高斯噪声 | 0 | 0.34 |
| 维纳滤波 | 0 | 0.01 |
| 中心剪切 1 | 0 | 0.1 |
| 中心剪切 2 | 0 | 0.11 |
| 直方图均衡 | 0 | 0 |


(a)高斯噪声攻击　(b)Vlener 滤波攻击　(c)随机剪切 1　(d)随机剪切　(e)直方图均衡

图 5　非标准攻击下的检测性能

(下转第 298 页)

Educational Technology & Society, 2006, 9 (2): 4～18
4 Aroyo L, Dicheva D, Cristea A. Ontological support for web courseware authoring. In: Proceedings of ITS'02, Biarritz, France, 2002
5 Aroyo L, Pokraev S, Brussee R. Preparing SCORM for the Semantic Web. On The Move to Meaningful Internet Systems 2003: CoopIS, DOA, and ODBASE, LNCS 2888. 621～634
6 Dolog P, Henze N, Nejdl W, Sintek M. Personalization in Distributed e-Learning Environments. In: Proceedings of the 13th International World Wide Web Conference, New York, USA, 2004
7 Dolog P, Henze N, Nejdl W, Sintek M. Towards the Adaptive Semantic Web. In: Principles and Practive of Semantic Web Reasoning (PPSWR'03), Mumbay, India, December 2003
8 周竹荣，吴敬花，邱玉辉. 基于概念图的网络课件与资源库集成. 计算机应用，2005，25(10)：2302～2305
9 Sintek M, Decker S. TRIPLE-A Query, Inference, and Transformation Language for the Semantic Web. International Semantic Web Conference (ISWC), Sardinia, June 2002
10 Resnik O. Semantic Similarity in a Taxonomy: An Information-Based Measure an its Application to Problems of Ambiguity and Natural Language. Journal of Artificial Intelligence Research, 1999,11:95～130

(上接第 256 页)

表 2 标准攻击下的检测结果对比

| 攻击典型 | 改进后方案<br>改进前方案 | 检测错误率<br>检测错误率 |
|---|---|---|
| 高斯滤波 3×3 | 0 | 0 |
| 高斯滤波 3×3 | 0 | 0 |
| 尖锐化 | 0 | 0 |
| PEO | 0 | 0 |
| 10%JPEG 压缩 | 0.20 | 0.26 |
| 15%JPEG 压缩 | 0.03 | 0.06 |
| 20%JPEG 压缩 | 0 | 0 |
| 缩放 0.75 倍 | 0 | 0 |
| 缩放 0.9 倍 | 0 | 0.27 |
| 缩放 1.5 倍 | 0 | 0.07 |
| 缩放 2.0 倍 | 0 | 0.06 |
| 朝 x 方向缩放 0.8 倍 | 0 | 0.15 |
| 朝 x 方向缩放 1.2 倍 | 0 | 0.09 |
| 朝 y 方向缩放 0.8 倍 | 0 | 0.14 |
| 朝 y 方向缩放 1.2 倍 | 0 | 0.08 |
| （续表） | | |
| 去除 17 行 5 列 | 0 | 0.22 |
| 去除 5 行 17 列 | 0 | 0.20 |
| 去除 5 行 1 列 | 0 | 0.10 |
| 去除 1 行 5 列 | 0 | 0.14 |
| 顺时针旋转 0.25"+剪切 | 0.14 | 0.31 |
| 逆时针旋转 0.25"+剪切 | 0.18 | 0.26 |
| 顺时针旋转 0.25"+剪切+缩放 | 0.08 | 0.26 |
| 逆时针旋转 0.25"+剪切+缩放 | 0.18 | 0.29 |
| 线性几何变换 (1,013,0.0008,0.011,1.008) | 0.40 | 0.42 |
| 随机几何弯曲 | 0.52 | 0.56 |
| 剪切 1% | 0.43 | 0.45 |
| shearing-x-0%-y-1% | 0.28 | 0.43 |
| shearing-x-1%-y-0% | 0.26 | 0.41 |
| shearing-x-1%-y-1% | 0.39 | 0.41 |

从表 1 和表 2 中可以看出：改进后的方案与改进前的方案相比，改进后的方案比改进前的方案在抵抗各种标准攻击和非标准攻击方面都有了明显的改善，尤其是在高斯白噪声攻击下对改进前方案鲁棒性的改善最大。这里所加的高斯白噪声较强，因为在这种较强的高斯噪声的干扰下，而且当嵌入容量较大时，会改进前水印方案的鲁棒性。除此之外，随机剪切对改进前的影响也较大，这也是因为这种剪切方式对 DCT 系数的影响较大的缘故。

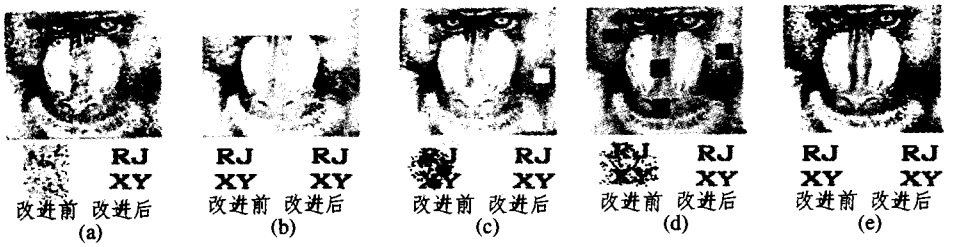

(a)原始图像 256×256　(b)加强了标志位的图像　(c)原始 LOGO

图 4 嵌入水印的图像

实验结果表明，特别是在高斯噪声影响下，改进后的方案明显优于原方案。

## 参 考 文 献

1 张春田，苏育挺. 信息产品的版权保护技术——数字水印. 电信科学，1998，14(12)：15～17
2 茹国宝，杨锐，夏双奎. 基于 Turbo 码的图像数字水印技术. 武汉大学学报(理学版)，2003，49(5)：633～636
3 Dong P, Galatsanos N P. Affine Transformation Resistant Watermarking Based on Image Normalization[J]. In: Image Pro International Conference, 2003 (3): 24～28
4 杨东林，叶梧. Turbo CDMA 多用户检测的研究. 电子科技大学学报，2002，29(3)：247～251




(a)高斯噪声攻击　(b)Vlener 滤波攻击　(c)随机剪切 1　(d)随机剪切　(e)直方图均衡

图 5 非标准攻击下的检测性能