

# 一种基于四叉树和变换域的渐进水印方案实现

李敏<sup>1</sup>, 周巍<sup>2</sup>

(1. 广东工业大学 计算机学院, 广东 广州 510090;

2. 深圳中兴通讯股份有限公司, 广东 深圳 518004)

**摘要:**数字图像、音频和视频等多媒体数字产品愈来愈需要一种有效的版权保护方法。数字水印技术则为上述问题提供了一个有效的解决方案。数字水印技术将数字、序列号、文字、图像标志等版权信息嵌入到多媒体数据中,以起到版权保护、秘密通信和产品标识等作用。文中针对 JPEG2000 的渐进压缩编码特性,利用四叉树编码算法和变换域数字水印算法在 JPEG2000 中实现了一种渐进水印方案。此方案在 VC6.0 中实现,根据实验结果,证明该方法是有效的并且对原有的 JPEG2000 编解码过程基本没有增添复杂度。

**关键词:**JPEG2000;数字水印;渐进分级编码;四叉树编码

**中图分类号:**TP309

**文献标识码:**A

**文章编号:**1673-629X(2006)05-0115-03

## Implementation of a Progressive Digital Watermark Based on Quadtree and Transformation Field

LI Min<sup>1</sup>, ZHOU Wei<sup>2</sup>

(1. Faculty of Computer, Guangdong University of Technology, Guangzhou 510090, China;

2. Shenzhen Zhongxing Telecommunication and Electron Co. Ltd, Shenzhen 518004, China)

**Abstract:** Multimedia digital products, such as digital image, audio and video need a more efficient method for copyright protection. The watermark technology provides an efficient solution to these kinds of issues. The digital watermark technology embeds digitals, serial numbers, words and image logs into multimedia database in order to protect copyright information, secrete communication and product identifier, etc. A method to realize progressive digital watermark in JPEG2000 is introduced and the method is suitable for the character of progressive coding in JPEG2000. The method adapts the algorithm of coding of quadtree and the algorithm of transformation field. It is realized in VC6.0 and is proved to be effective by the experiment results.

**Key words:** JPEG2000; digital watermark; progressive coding; coding of quadtree

### 0 引言

JPEG2000 标准由联合图像专家组于 2000 年颁布,作为 JPEG 标准的一个更新换代标准,具有渐进压缩编码、感兴趣区域编码、码流的随机访问和随机截取、无损压缩和有损压缩统一并可调等特性<sup>[1,2]</sup>。

随着多媒体技术的飞速发展,对多媒体内容的版权保护成为迫切需要的课题,从而产生了数字水印技术。数字水印技术将与多媒体内容相关或不相关的信息直接嵌入多媒体内容当中,但不明显影响原内容的价值,并不能被人的知觉系统觉察到,却能够通过专用工具来提取这些隐藏信息。数字水印技术一般要求具有隐蔽性、隐藏位置的安全性、鲁棒性。

在 JPEG2000 标准逐渐被社会所接受并被极力推广之际,实现 JPEG2000 中的数字水印技术,对采用

JPEG2000 编码的图像的知识产权保护具有重要的实际意义。

### 1 渐进水印的实现方案

常见的水印算法有:最低有效位算法、Patchwork 算法、纹理块映射编码算法、文本微调算法、变换域数字水印算法、直接序列扩频水印算法<sup>[3,4]</sup>。其中变换域数字水印算法由于比较好地利用了图像在频率域中能量分布特性对图像质量的影响较小的特点,比如 DCT 变换域数字水印算法广泛应用于 JPEG 以及 MPEG、H26X 系列图像标准中,因此获得了很大的成功。鉴于此,文中采用了小波变换域上的数字水印算法,在具体的嵌入上采用了最低有效位算法。

但是 JPEG2000 对图像的处理是渐进的,从而极易在只对图像的基本级进行解码时抹去水印或者将水印变得模糊不清。针对这种情况,提出了一种渐进水印方案,即水印根据图像解码的效果而不断变化。为了实现水印的

收稿日期:2005-11-22

作者简介:李敏(1978-),女,湖北人,助教,硕士研究生,研究方向为图像处理、数据通信与网络技术。

渐进性,采用四叉树编码方案来实现水印的渐进编码。四叉树编码的压缩比并不大但复杂度很低,比较适合于简单水印的渐进编码。

### 1.1 二值图像的四叉树表示方式

普通图像的四叉树压缩算法思想是把图像四等分,然后根据每个子图的像素值决定是否再进行四等分,如果不再等分则记录该子图的平均像素值,如此循环直到图像被完全划分,从而依据四叉树的不同层进行解码就可以实现图像的分级<sup>[5~7]</sup>。

设图像的宽度为  $w$ , 高度为  $h$ , 不失一般性, 令  $w \geq h$ ,  $m$  为满足  $2^m < w$  的最大整数, 那么以  $2^m$  作为边长把图像划分四个子图。对于尺度不足的子图也作为一个子图, 对于不存在的子图则作为空枝并记为  $-1$ 。然后对每个非空子图再逐次以边长  $2^{m-1}, 2^{m-2}, \dots, 2^0$  进行划分, 一直到每个子图不能再划分为止。在每次划分的时候, 都要考察当前子图的所有像素值是否比较均匀, 如果均匀则不再划分, 并把当前子图所对应的树结点记为  $0$ , 同时记下此时的像素平均值, 否则记为  $1$ 。显然, 只要给定图像的宽高以及每个点的像素值, 那么图像对应的四叉树则确定了; 反过来, 只要四叉树确定了, 则可以逆推出图像数据。四叉树的结构数据保存采用广度优先方法而对应的图像数据采用自上而下、从左到右, 先保存结点类型为  $0$  的结点对应的图像数据, 然后再保存结点类型为  $1$  的结点对应的图像数据。

当原始四叉树构建完毕后, 就开始判定各个结点的类型, 这通过递归的方法来实现, 即从一个像素所代表的最小子图开始逐渐合并直到全图只有一个子图为止。用两个变量来控制四叉树中间结点和叶结点的形成, 一个是表示子图的像素平均值与上一层子图的所有像素值的平均值的均差阈值  $\text{DifferenceE}$ , 另一个是四叉树每层所需要的误差递减量  $\text{DecreaseE}$ 。当均差大于阈值时, 构造四个叶结点和一个上层中间结点, 否则数据留待上层继续运算。

二值图像的四叉树编解码与普通图像的四叉树相同, 但是对应的子图像素平均值的计算方式不同, 遵循如下规则:  $n\text{NodeValue} = 0$ , 均值  $= 0$ ;  $n\text{NodeValue} = 1$ , 均值  $= 1$ ;  $n\text{NodeValue} = 2$ , 均值  $< 0.5$  且  $> 0$ ;  $n\text{NodeValue} = 3$ , 均值  $\geq 0.5$  且  $< 1$ 。从而可以实现二值图像的四叉树的结构数据与像素数据的一起表示, 而且由于  $n\text{NodeValue}$  的取值为  $0, \dots, 3$ , 所以可以把每四个值合为一个字节。对于图 1 所示的二值图像的对应四叉树表示如图 2 所示, 对应的存储方式表示如图 3 所示, 注意黑点的像素值为  $0$ , 白点的像素值为  $1$ 。

由于在形成结点时采用了取子图平均值的做法, 所以可以根据压缩比的要求来决定是否放弃对低层数据的保存, 即压缩比可以人为控制。四叉树的不同层次的数据对应着像素之间的变化情况, 层次越低表示数据变化越快, 层次越高代表数据在较大范围内都没有变化, 因此四叉树的层次又与图像的变化频率相关, 上层代表低频数据, 下

层代表高频数据。当为了获得较高的压缩比时, 可以采用牺牲高频数据的办法; 如果为了保证完全无损压缩, 则需要保留所有的高频数据。

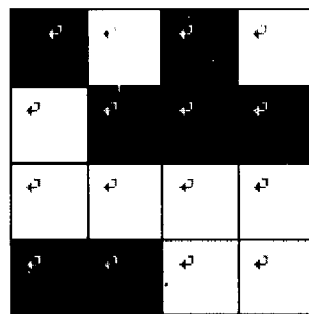


图 1 示例二值图像的像素取值

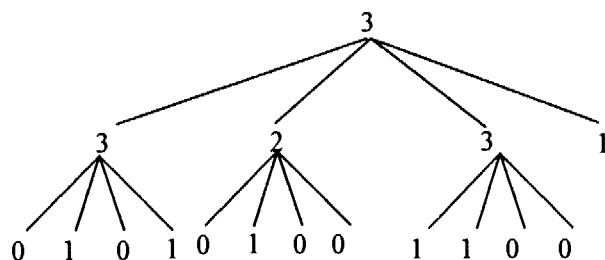


图 2 示例二值图像的对应四叉树结构图

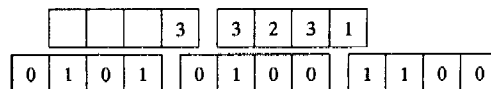


图 3 示例二值图像的对应四叉树结构存储示意图

### 1.2 水印嵌入和提取的具体实现

目标图像的选择是随意的, 但水印的选择规定为二值图像, 主要是为了减少水印信息量从而减少对目标图像的影响。其实对于灰度图像或彩色图像作水印的情况也测试过, 只是要求目标图像比较大或者水印图像比较小也可以。在此方案中, 水印嵌入的主要思想是将目标图经 JPEG2000 编码器预处理后经小波变换得到小波系数, 然后将压缩处理得到的水印嵌入到小波系数中。水印提取的主要思想是 JPEG2000 解码器对码流预处理后得到小波系数, 然后将水印从小波系数中提取出来。

在小波变换后, 首先从最基本的低频子带开始逐次扫描小波系数, 将水印信息位串按照每两个比特一次嵌入到适宜的小波系数的低比特位中, 水印的加入顺序为基本的水印信息嵌在最基本的低频子带的小波系数中, 细节水印信息嵌在相对高频子带中。在小波反变换后, 首先从最基本的低频子带开始逐次扫描小波系数, 并从小波系数的低比特位中提取水印信息, 在提取的同时进行水印解码。如果水印解码完毕, 而小波系数的扫描仍然没有结束, 表示水印信息完全嵌入到原图像中; 如果小波系数的扫描完毕, 而水印解码仍然没有结束, 表示水印信息没有完全嵌入到原图像中。

注意: 首先, 水印的嵌入并不是完全依照小波系数的顺序逐一嵌入, 而是水印的不同层次的码流嵌入到目标图像的 JPEG2000 码流的对应层次中, 当然嵌入在同一层中

的水印码流是依照小波系数逐一嵌入的;其次,水印不一定要完全嵌入,也不一定要完全提取,是否完全嵌入与提取只会影响水印的清晰度,这是渐进水印的一种优势;另外,如果编码过程中有量化的过程,那么水印的嵌入应在小波变换和量化后进行,同理,水印的提取应在反量化和小波反变换前进行。

2 实验结果

根据上述实现方案流程,利用 VC6.0 实现了本方案一个完整程序。以图 4 所示的 256×256 的灰度 Lena 为例,JPEG2000 的量化方案为最低一层的子带的所有比特平面全部编码,而对以后的每层子带不进行编码的比特平面逐层加 2,采用 5/3 小波。图 5 为没有加入水印的压缩效果图,图 6 为加入了水印的压缩效果图。图 5 和图 6 的客观评价参数比较如表 1。



图 4 256×256 的灰度 Lena



图 5 没有加入水印的压缩效果图 图 6 加入了水印的压缩效果图

表 1 图 5、图 6 的客观评价参数比较

性能\图像	图 5	图 6
大小(字节)	8489	8464
压缩比	7.847096	7.870274
峰值信噪比	33.507068	33.033931
均方误差根	5.385013	5.686482
编码时间(ms)	67.807	67.887
解码时间(ms)	44.414	44.654

从图 5 和图 6 可以明显地看出两图基本没有区别,从它们的客观参数也可以印证这一点。当然加了水印后的

客观评价参数会比没有加水印时低些,但是减小幅度非常小,而且编解码的时间也几乎没有改变。图 8 为从图 7 中提取出来的水印(自左至右分别为从第一层到第四层码流中提取出来的水印效果图),可以直观看出水印的效果具有逐渐清晰的渐进效果。提取出来的水印没有噪声,这是因为在编码时嵌入了水印信息的比特平面数据与解码后得到的比特平面数据是一致的,所以不会有噪声,只会在渐进过程中有模糊效果。



图 7 原始水印



图 8 从图 7 中提取出来的水印

3 结束语

在此方案中,由于水印信息首先是嵌在小波系数的低比特位中,从而对图像的影响很小;小波变换具有全局性的统计意义,对任何小波系数的修改都会平衡到整个图像中而不易形成噪声,在这一点上,小波域上的水印叠加比 DCT 域上的水印叠加要优越得多;时间复杂度很低,基本没有添加时间复杂度,这点可以从表 1 提供的编解码时间项中得到验证。由于 JPEG2000 对图像是分级压缩的,而低频小波系数正好代表了图像的基本轮廓和基本信息,所以水印的基本信息正好加在图像的基本轮廓中而不易被 JPEG2000 编解码器去掉,因此本方案对于 JPEG2000 具有一定的鲁棒性。

渐进水印方案比较好地适应了 JPEG2000 的渐进压缩编码特性,在图像载体和水印的选择上具有非常大的灵活性,可以适应各种场合的需要,对采用 JPEG2000 编码的图像的知识产权具有良好的保护作用。

参考文献:

[1] ISO/IEC 15444. Information technology JPEG2000 image coding system:Part 1 Core coding system[S]. 2000.  
[2] 丁贵广,郭宝龙.新一代静止图像压缩编码标准:JPEG2000 概述[J].计算机与信息技术,2002(3):29-33.  
[3] Ruanaidh J O,Pun T. Rotation, scale and translation invariant digital image watermarking[A]. in Proceedings IEEE International Conference on Image Processing 1997 (ICIP 97) [C]. Santa Barbara,CA, USA:[s. n. ],1997. 536-539.  
[4] Swanson M D,Kobayashi M, Tewfik A H. Multimedia data embedding and watermarking technologies[J]. Proceedings of the IEEE,1998,86(6):1064-1087.

c. 防止重访攻击:SSL 协议记录层为每一个上层消息做 MAC 验证时,加入了消息序列号,这不仅可以防止对记录层消息的重放攻击,还可以使消息免遭延迟、重排和删除。消息序列号为 64 位,不会溢出。每个连接上的两个方向上的序列号被独立保存。

## 4 系统演示及效率分析

### 4.1 实际运行演示

系统的运行界面如图 1 所示。

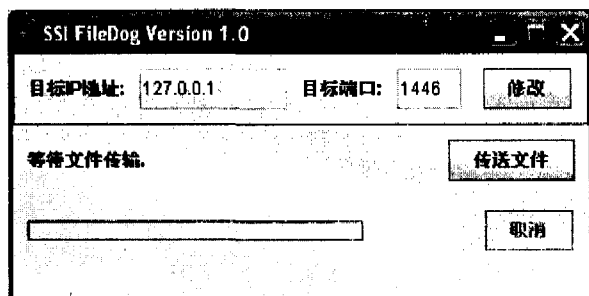


图 1 系统界面

传输文件前设置好目标地址和端口,然后点击传送文件即可选择要传输的文件。当有文件需要接受时,系统会自动弹出信息窗口,显示文件的源地址和文件名,并询问是否接收。用户的使用过程中数据的加密解密等对用户来说是透明的,用户无需关心数据如何加密、何时解密等底层问题。

### 4.2 加密传输效率分析

采用了对比的方法分析 SSL 安全套接字扩展的实际传输效率。通过与未加密的文件传输器对比传输速度来分析实际应用中的加密效率。为了保证对比的结果具有可比性,普通的文件传输器除了使用普通的 socket 传输外,其他代码和加密的版本一样。

测试中使用的测试文件大小从 6kB~72MB 不等递增,每个文件均传输五次,取五次传输速度的平均值(测量单位:ms),结果如表 1。

通过对比表 1 发现:

a. 加密传输所需的加密时间随着传输文件大小的增加而增加;

b. 随着文件大小的增加,加密传输时间增加的速度和无加密传输时间增加的速度基本一致。

通过以上分析可以知道使用 SSL 加密传输在效率上是可行的。实际应用中在传输大小小于 10MB 的文件时,加密传输所需加密时间是很小的,对传输没有很大的影响。而文中设计的文件传输器正是为了传输加密的公文、

电子合同等商务政务方面的小文件。所以传输效率方面是完全可以满足应用需求的。

表 1 效率比较

文件大小	无加密	SSL 加密
6kB	2ms	3.2ms
117kB	15.6ms	24.8ms
777kB	156.4ms	200ms
1.6MB	249.8ms	368.6ms
6.74MB	756.2ms	1406.2ms
72MB	8668.6ms	11299.8ms

## 5 结束语

主要介绍了基于 SSL 协议的安全文件传输器的实现原理,以及对于 Java JSSE 的应用。基于 SSL 协议的文件传输器直接应用了 SSL 协议这种结构严谨、安全的协议,大大简化了安全文件传输的底层设计难度。此外体现出了 Java JSSE 包对于 SSL 协议很好的封装性,对于底层复杂的加密签名等算法进行了很好的包装隐藏,使得开发者能够轻松应用其 API 实现基于 SSL 协议的数据加密传输。在提供了很好的易用性的同时,JSSE 还提供了强大的可扩展性,使得人们可以轻松定制各种加密签名的细节。但是由于美国对出口密码产品的管制和编程中某些 SSL/TLS 协议不当的用法,系统还是存在面临攻击的危险<sup>[3]</sup>,如穷尽搜索 40 位 RC4 密钥攻击、利用 RSA PKCS#1 编码方法的脆弱性获得 pre-master-secret 的攻击等危险、拒绝服务攻击等<sup>[5]</sup>。此外可以看出 SSL/TLS 协议的传输效率是完全可以满足 10MB 以下小文件传输的。

### 参考文献:

- [1] Apostolopoulos G, Peris V, Saha D. Transport Layer Security How much does it really cost[A]. INFOCOM '99. Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings[C]. [s. l.]: IEEE, 1999. 717-725.
- [2] Rescorla E. SSL 与 TLS[M]. 北京:中国电力出版社,2002.
- [3] Gong L, Ellison G, Dageforde M. 深入 Java 2 平台安全——体系架构、API 设计和实现(第 2 版)[M]. 北京:电子工业出版社,2004.
- [4] 卿斯汉. 安全协议[M]. 北京:清华大学出版社,2005.
- [5] 王克苑,张维勇,王建新. SSL 安全性分析研究[J]. 合肥工业大学学报(自然科学版),2004,27(1):87-91.

(上接第 117 页)

- [5] Hamzaoui R, Ganz B, Saupe D. Quadtree based variable rate oriented mean shapegain vector quantization[A]. Storer J A, Cohn M. in: Proceedings DCC'97 Data Compression Conference[C]. [s. l.]: IEEE Comp Soc Press, 1997. 327-336.

- [6] Lin T W. Compressed quadtree representations for storing similar images[J]. Image Vision Computing, 1997, 15(11): 833-843.
- [7] 魏为民. 基于彩色静止数字图像的信息隐藏技术研究[J]. 计算机应用与软件, 2002(11): 52-54.