

结合近似最优比特分配的改进 SPIHT 算法

潘志刚¹, 张文超¹, 王晓晨²

(1. 中国科学院电子学研究所, 北京 100080; 2. 合肥工业大学电气与自动化工程学院, 合肥 230009)

摘要: SPIHT 算法是一种实用、高效的小波零树图像编码算法。针对 SPIHT 算法存储空间需求大、运算复杂度较高等缺点, 提出了一种改进的快速、低存储 SPIHT 算法, 该算法将小波变换所形成的水平、垂直、对角和低频 4 个子带分成 4 个处理单元, 对每个处理单元分别进行量化编码, 并在各单元之间采取近似最优比特分配以提高量化性能。实验结果表明, 改进算法在提高峰值信噪比等性能指标的同时, 有效地减少了算法的存储需求及运算时间。

关键词: 图像编码; 小波变换; 零树量化; SPIHT; 比特分配

Improved SPIHT Algorithm Combined with Nearly Optimal Bit Allocation

PAN Zhi-gang¹, ZHANG Wen-chao¹, WANG Xiao-chen²

(1. Institute of Electronics, Chinese Academy of Sciences, Beijing 100080;

2. School of Electric Engineering and Automation, Hefei University of Technology, Hefei 230009)

【Abstract】 SPIHT(set partitioning in hierarchical tree) algorithm is a wavelet based zerotree image encoding algorithm known for its high efficiency. However, its high memory requirement and long execute time consumption are obstacles to implement real-time compression. This paper presents a new fast and low memory image zerotree encoding algorithm. This algorithm processes wavelet coefficients of horizontal, vertical, diagonal and low frequency subband respectively, and a nearly optimal bit allocation stage is applied in the above subband to get better compression performance. Experimental results show this algorithm outperforms the original SPIHT algorithm in PSNR and efficiently reduces both the memory requirement and the time consumption.

【Key words】 image encoding; wavelet transform; zerotree quantization; set partitioning in hierarchical tree (SPIHT); bit allocation

1 概述

自 20 世纪 80 年代末期 S.Mallat 将快速小波变换引入到图像处理以来, 小波变换以其优异的时频局部化能力和良好的去相关能力在图像压缩领域得到了广泛的应用, 并取得了良好的效果。1993 年, J.M.Shapiro^[1]利用小波变换在不同分解级之间的自相似性, 提出了基于比特连续逼近的嵌入零树小波编码算法(embedded zerotree wavelet, EZW), 成为基于小波的静态图像压缩领域的重大突破。1996 年, 由 A.Said 和 W.A.Pearlman^[2]提出的 SPIHT(set partitioning in hierarchical tree)算法是对 EZW 算法的改进, 它以 EZW 算法的零树结构为基础, 但是具有更高的压缩效率, 相同比特率下, 即使不需要熵编码环节, SPIHT 也总能取得优于 EZW 的量化性能。

但是通过深入分析 SPIHT 算法流程, 可以发现该算法还存在以下几方面不足: (1) 编码过程需要占用大量内存, 尤其在压缩比特率较高时, 表现更为明显; (2) 该算法的扫描方式使得所有子带的编码交叉进行, 因此任一子带的误码将影响到其他子带, 使得后续的解码无法进行; (3) 该算法对各子带编码使用统一阈值, 这将造成个别子带额外的重要系数冗余扫描和输出比特数, 从而有损编码效率。

针对 SPIHT 算法存储空间需求大, 不利于硬件实现等缺点, 文献[3]提出了 LZC(listless zerotree coding)算法, 该算法利用 2 个标志位图代替原来的 3 个集合列表, 极大地降低了内存需求, 但却在一定程度上降低了编码器性能。文献[4]提出了 NLS(no list SPIHT)算法, 该算法以 SPIHT 零树结构及

其分割策略为基础, 通过采用状态表来记录集分割和编码信息, 严格按照广度优先顺序进行零树重要性测试, 有效降低了内存需求, 量化性能比原始 SPIHT 算法性能略低。文献[5]引入了“误差位数”、“绝对零点”和“绝对零树”的概念并将之用于 SPIHT 的编码当中, 该算法能够有效地降低算法的存储需求和运算时间, 但压缩性能指标也随之降低, 而且针对不同类型图像不具有广泛适用性。

本文提出了一种改进的快速、低存储 SPIHT 算法, 该算法将小波变换所形成的水平、垂直、对角和低频 4 个子带分成 4 个处理单元, 对每个处理单元分别采用修正的 SPIHT 算法进行量化编码, 并在各单元之间按照率失真准则进行近似最优比特分配以提高量化性能, 在一定程度上克服了 SPIHT 算法所存在的不足并提高了压缩性能。

2 改进的 SPIHT 算法

2.1 改进算法基本原理

图像经小波变换之后, 各子带系数能量并不相同, 若对各子带进行同等重要的编码, 则方差较大的子带系数, 其量化失真也较大, 必然使总的量化性能降低。因此可以在不同子带之间寻求一种合理的比特分配方式, 使得量化性能达到或接近最优。本文的改进思路在于, 放弃原算法嵌入式编码

作者简介: 潘志刚(1976 -), 男, 博士、助理研究员, 主研方向: 遥感图像处理, 小波分析及信源编码; 张文超, 博士研究生; 王晓晨, 博士、讲师

收稿日期: 2006-08-10 **E-mail:** pan0912@163.com

的特点,对小波变换所形成的 LL、HL、LH、HH 4 个子带划分成如图 1 所示的 4 个处理单元,对每个单元分别进行量化编码,同时在各单元之间进行比特分配以提高量化性能。以图 1 所示三阶小波变换为例,改进算法的实现描述如下:

(1)处理单元划分。把小波变换系数划分成如图 1 所示的 4 个处理单元。

(2)比特分配。针对特定的压缩比特率,利用自适应比特分配算法给 LL、HL、LH、HH 这 4 个单元分配相应的量化比特数。

(3)系数分类与编码。对于 LL 单元,因其只有元素信息,不存在集合,可以省去 LIS 列表,编码时首先将每一小波系数与阈值比较,如果重要则移入 LSP 中,否则移入 LIP 中;其细化过程同原始 SPIHT 算法。对于 HL、LH、HH 三单元,分别采用原始 SPIHT 算法进行编码。

(4)对生成的码流按照特定格式打包传输。由此可见,改进算法的核心在于第(2)步中比特分配的实现。

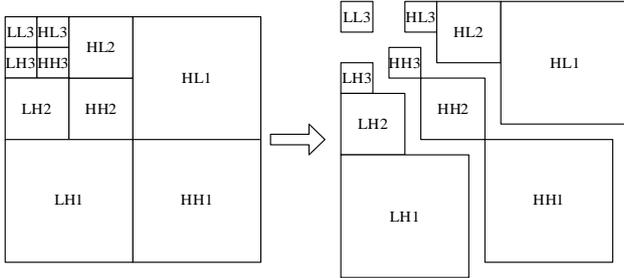


图 1 处理单元划分及对应的小波系数

2.2 比特分配

实现编码过程全局最优的比特分配是一个有约束优化问题,目前典型的方法有:采用分治策略的二分法搜索^[6],动态规划法^[7]以及率失真曲线估计法^[8]。上述比特分配方法从本质上来讲均需要计算各种量化条件下的失真,因此必然会导致计算复杂性的增加。根据率失真理论,提出一种较为简单的近似最优快速比特分配方法,该方法对于本文的改进算法能够取得较好的结果,具体的比特分配过程如下。

假设对一二维信号进行 5 阶小波分解,并经过处理单元划分,得到 LL、HL、LH、HH 4 个子带分量,如图 1 所示。令 η_n 表示单个子带内系数数目与总的系数数目的比值,有

$$\sum_{n=0}^3 \eta_n = 1 \quad (1)$$

根据正交小波变换的能量守恒性,重建信号的失真等于小波域内系数的量化失真,所以,信号的平均量化失真为

$$D_T = \sum_{n=0}^3 \eta_n D_n(R_n) \quad (2)$$

对于非高斯或者有记忆信源,其失真率函数 $D(R)$ 满足^[9]

$$D_L(R) = Q \cdot 2^{-2R} \leq D(R) \leq D_G(R) \quad (3)$$

式中, $D_L(R)$ 被称为 Shannon 失真率下限, $Q = \frac{1}{2\pi e} 2^{2h(X)}$ 为熵功率, $h(X)$ 为微分熵。当量化速率很高时,信源的实际失真率函数逼近 $D_L(R)$, 所以,在低比特率量化条件下,可以取 $D(R) = Q \cdot 2^{-2R}$, 此时式(2)可改写为

$$D_T = \sum_{n=0}^3 \eta_n Q_n \cdot 2^{-2R_n} \quad (4)$$

对于 LL 子带,因其不满足低比特率量化条件,所以考虑除 LL 子带之外的局部最优比特分配问题,由式(1)可知,LL 子带系数所占分量很小,对总体量化性能的影响并不大,考虑到实际失真率函数与其下限的逼近误差,引入加权系数,则式(4)修正为

$$D_T = \frac{1}{3} (w_{HL} Q_{HL} \cdot 2^{-2R_{HL}} + w_{LH} Q_{LH} \cdot 2^{-2R_{LH}} + w_{HH} Q_{HH} \cdot 2^{-2R_{HH}}) \quad (5)$$

总的量化比特率 R_T 满足

$$R_T = \frac{1}{3} (R_{HL} + R_{LH} + R_{HH}) \quad (6)$$

最优比特分配问题可描述为:当 R_T 一定时,使得式(5)所定义的平均量化失真为最小。使用拉格朗日乘数法来求解上述最小化问题,需建立目标函数

$$\arg \min_{R_n} J = \arg \min_{R_n} \left[D_T + \lambda \left(R_T - \frac{1}{3} (R_{HL} + R_{LH} + R_{HH}) \right) \right] \quad (7)$$

联立式(6),求解方程组

$$\begin{cases} \frac{\partial J}{\partial R_{HL}} = 0, & \frac{\partial J}{\partial R_{LH}} = 0, & \frac{\partial J}{\partial R_{HH}} = 0 \\ R_T = \frac{1}{3} (R_{HL} + R_{LH} + R_{HH}) \end{cases} \quad (8)$$

可得

$$\begin{aligned} R_{HL} &= R_T + \frac{2}{3} h(X_{HL}) - \frac{1}{3} [h(X_{LH}) + h(X_{HH})] + \frac{1}{6} \log_2 \left(\frac{w_{HL} w_{HL}}{w_{LH} w_{HH}} \right) \\ R_{LH} &= R_T + \frac{2}{3} h(X_{LH}) - \frac{1}{3} [h(X_{HL}) + h(X_{HH})] + \frac{1}{6} \log_2 \left(\frac{w_{LH} w_{LH}}{w_{HL} w_{HH}} \right) \\ R_{HH} &= R_T + \frac{2}{3} h(X_{HH}) - \frac{1}{3} [h(X_{HL}) + h(X_{LH})] + \frac{1}{6} \log_2 \left(\frac{w_{HH} w_{HH}}{w_{HL} w_{LH}} \right) \end{aligned} \quad (9)$$

式(9)中,加权系数的选取规则如下:对于计算出的子带系数熵 $h(X_{HL})$ 、 $h(X_{LH})$ 、 $h(X_{HH})$,求其最大值并设为 h_{\max} ,则子带加权系数的值可由式(10)求出

$$w_{mn} = h_{\max} / h(X_{mn}) \quad (10)$$

经过大量实验表明,对于以 8bit 存储的一般光学图像,当总的量化比特率为 $0.2 \leq R_T \leq 1.0$ 时,LL 子带的量化比特率可取为 $10 \leq R_{LL} \leq 11$,此时 R_{LL} 的变化对量化性能的影响非常小。对某一确定 R_{LL} , R_{HL} , R_{LH} , R_{HH} 的值,计算相应的量化比特数分别为 N_{LL} , N_{HL} , N_{LH} , N_{HH} ,此时 N_{LL} 为多出的比特数,需做如下处理:判断 N_{HL} , N_{LH} , N_{HH} 三者中的最大值并减去 N_{LL} 。

3 实验结果与分析

算法选择 CDF9/7 小波并进行 5 阶分解与重构。以 $512 \times 512 \times 8$ bit 的 JPEG 标准测试图像 Lena、Barbara、Goldhill 为例,从压缩性能、最大存储需求、运算时间等 3 个方面将改进算法(MSPIHT)与原始 SPIHT 算法进行比较(考虑到算法的实时性要求,改进算法与原始算法均省略了熵编码环节),所得实验结果分别如表 1、表 2 所示。

表 1 不同码率下重构图像的峰值信噪比 (dB)

rate	Lena		Barbara		Goldhill	
	MSPIHT	SPIHT	MSPIHT	SPIHT	MSPIHT	SPIHT
0.2	31.85	31.56	25.46	25.45	28.62	28.60
0.4	35.22	35.08	29.17	28.91	31.30	31.24
0.8	38.56	38.48	33.75	33.65	34.49	34.47
1.0	39.70	39.75	35.56	35.52	35.53	35.56

表 2 中间数组最大存储容量及运算时间比较(Lena 图像)

rate	MSPIHT		SPIHT	
	最大存	运算时间/s	最大存储	运算时间/s
0.2	10612	2.96	19572	3.98
0.4	17575	5.89	39392	10.57
0.8	30285	13.39	78245	42.37
1.0	33943	20.59	78245	63.79

图 2 给出了当码率为 0.2bit/s 时的解压缩重构图像,参数 CR 表示压缩比。



图2 解压缩数据重构图像

由表1所示数据可以看出,通过比特分配,可以使改进算法的峰值信噪比指标总体上略优于原算法。表2中最大存储量表示为LSP、LIP和LIS3个中间数组的最大长度之和,运算时间表示为在Matlab6.5下运行该程序时编码器所需要的最大时间。由表中数据可知,改进算法与原算法相比,能够明显降低3个中间数组的最大长度,约为原算法的1/2;同时编码器的运算时间与原算法相比,也有明显的降低。SPIHT算法的存储量主要体现为LSP、LIP和LIS3个数组的大小变化,这说明改进算法在运算时间与最大存储需求方面与原算法相比有较明显改进。同时改进算法对4个处理单元分别进行处理,对于硬件来说更容易并行实现,从而可以进一步减少算法的执行时间,缺点是总的存储需求与串行实现相比要增加很多。

4 结束语

本文针对SPIHT算法存储空间需求大、运算复杂度较高等缺点,提出一种改进的快速、低存储SPIHT算法,该算法将小波变换所形成的水平、垂直、对角和低频4个子带分成4个处理单元,对每个处理单元分别进行量化编码,并在各单元之间采取近似最优比特分配以提高量化性能。实验结果

(上接第14页)

所以,本文的可验证的加密的RSA签名是不可伪造的。

(3)签名的保密性。给定一个可验证的加密的RSA签名的密文 $C=(c_1, c_2, c_3)$,除了TTP和Alice之外,其他任何攻击者想要从 $C=(c_1, c_2, c_3)$ 中解密出Alice的签名,在计算上是不可行的。实际上,可验证的加密的RSA签名采用了标准RSA加密算法,其安全强度与RSA加密是一样的。所以,对一个攻击者来说,从 $C=(c_1, c_2, c_3)$ 解密出Alice的签名与攻击标准RSA加密一样困难。

对可验证的加密RSA签名的安全分析,实际上保证了基于该构件的公平交换协议RSAEP的安全性。它能保证第3节的协议RSAEP具有强公平性^[1]。

4.2 效率分析与比较

这里从计算和通信开销两个方面比较本文的协议与以前的相关协议。文献[1,2,3,5]中分别提出了交换RSA数字签名的公平交换协议,它们与本方案的比较如表3所示,这里假设RSA模长1024bits。从表中可以看出,RSAEP协议在计算开销方面都优于其他的方案。

表3 与相关协议的效率比较

协议处理	RSAEP Protocol	Zhou et al's Protocol ^[5]	Ateniese's Protocol ^[1]	Bao et al's Protocol ^[2]	Chen's Protocol ^[3]
协议中指数运算次数	9	10	16	>20	>26
争端解决协议中指数运算次数	6	3	11	5	11
可验证的加密签名比特长度	8 192	2 ¹³⁷	8 192	4 096	3 072

表明:改进算法的恢复图像质量及峰值信噪比略优于原算法并明显降低了算法的存储需求与运算时间。

参考文献

- Shapiro J M. Embedded Image Coding Using Zero Trees of Wavelet Coefficients[J]. IEEE Trans. on Signal Processing, 1993, 41(12): 3445-3462.
- Said A, Pearlman W A. A New Fast and Efficient Image Codec Based on Set Partitioning in Hierarchical Trees[J]. IEEE Trans. on Circuits and Systems for Video Technology, 1996, 6(3): 243-250.
- Lin W K, Burgess N. Low Memory Color Image Zerotree Coding[C]//Proceedings of the 32nd Asilomar Conference on Signal, Systems and Computer. 1998: 231-235.
- Wheeler W, Pearlman W A. SPIHT Image Compression Without Lists[C]//Proceedings of the IEEE ICASSP'00. 2000: 2047-2050.
- 孙勇, 胡广书, 张辉. 一种新的低存储量的图像零树编码算法[J]. 清华大学学报(自然科学版), 2001, 41(9): 59-62.
- Daubechies I, Sweldens W. Factoring Wavelet Transform into Lifting Steps[J]. J. Fourier Analysis and Applications, 1998, 4(3): 245-267.
- Prandoni P, Vetterli M. R/D Optimal Linear Prediction[J]. IEEE Trans. on Speech and Audio Processing, 2000, 8(6): 646-655.
- Shoham Y, Gersho A. Efficient Bit Allocation for an Arbitrary Set of Quantizers[J]. IEEE Trans. on Acoust. Speech, Signal Processing, 1988, 36(9): 1445-1453.
- 朱雪龙. 应用信息论基础[M]. 北京: 清华大学出版社, 2001: 229-233.

5 结论

公平交换协议是电子商务最重要的基础构件之一,它保证参与交易的双方都得到对方的商品,或都得不到对方商品的任何信息。由于网络本身有安全缺陷,因此设计安全、高效、实用的公平交换协议尤其重要。本文提出了一种新的基于整数扩环上的可验证的加密RSA签名,并基于该密码构件设计了一个公平交换协议。安全分析和效率比较表明,本文的方案安全且高效。

参考文献

- Ateniese G. Verifiable Encryption of Digital Signatures and Applications[J]. ACM Transactions on Information and System Security, 2004, 7(1): 1-20.
- Bao F, Deng R, Mao W. Efficient and Practical Fair Exchange Protocols with Off-line TTP[C]//Proceedings of IEEE Symposium on Security and Privacy. 1998-05: 77-85.
- Chen L. Efficient Fair Exchange with Verifiable Confirmation of Signatures[C]//Proc. of Advances in Cryptology(ASIACRYPT'98). 1998: 286-299.
- Rivest R L, Shamir A, Adleman L. A Method for Obtaining Digital Signatures and Public-key Cryptosystems[J]. Communications of the ACM, 1978, 21(2): 120-126.
- 周永彬, 张振峰, 卿斯汉, 等. 基于RSA签名的优化公平交换协议[J]. 软件学报, 2004, 15(7): 1049-1055.