

数字图像多重水印及容量分析

张帆^{1,2}, 刘亚丽³, 苏育挺¹, 张春田¹

(1. 天津大学电子与信息工程学院 天津 南开区 300072; 2. 河南大学先进控制与智能信息处理研究所 河南 开封 475001;
3. 河南大学教育科学学院 河南 开封 475001)

【摘要】利用CDMA系统多址复用的特点,提出了一种基于CDMA的多重水印算法,在小波变换域中同时嵌入多个水印。对多个原始水印进行卷积编码和交织编码后,采用Gold码组进行正交扩频,经CDMA编码的水印信息被叠加嵌入在除HH1以外的其他小波子带中。水印嵌入的幅值根据Watson小波域视觉感知模型确定。嵌入位置取决于一个PN序列随机发生器,检测时不需要原始图像。在此基础上对多重水印容量进行了分析,结果表明当嵌入两个水印时,其容量大于任何一个单一水印的容量,但小于两个单一水印容量之和。

关键词 容量; 码分多址; 数字水印; 小波变换
中图分类号 TP391.41 文献标识码 A

Multiple Watermarking and Capacity Analysis of Digital Image

ZHANG Fan^{1,2}, LIU Ya-li³, SU Yu-ting¹, ZHANG Chun-tian¹

(1. College of Electronic and Information Engineering, Tianjin University Lankai Tianjin 300072;
2. Institute of Advanced Control and Intelligent Information Processing, Henan University Kaifeng Henan 475001;
3. College of Education Science, Henan University Kaifeng Henan 475001)

Abstract According to the multiple accessing technique of Code Division Multiple Access (CDMA) system, multiple watermarks are encoded with convolution and interleaved in block. Orthogonal Gold sequences are used to spread spectrum of the copyright messages. CDMA encoded copyright messages are embedded into the wavelet sub-bands except HH1 sub-band. The embedded amplitude is decided by Watson's perceptual model of wavelet transform domain, and the embedded position in the selected wavelet sub-bands is decided randomly by a Pseudorandom Noise (PN) sequence. Watermarks are extracted without the need of original image. The capacity of proposed algorithm is also discussed. Experimental results show that proposed algorithm improves the detection Bits Error Rate (BER) and that multiple watermarks have preferable robustness and invisibility.

Key words capacity; code division multiple access; digital watermark; wavelet transform

多媒体信息的数字化为多媒体信息的存取提供了极大的便利,但副作用是有恶意的人有可能在没有得到作品所有者许可的情况下拷贝和传播有版权的内容,由此引发的盗版问题和版权纷争已成为严重的社会问题。多重水印技术是用来解决多著作权问题以及数字产品在发布、销售、使用等不同阶段的版权认证问题的有效手段。多重水印算法比单个水印算法有更多的技术要求,如多个水印信号在嵌入和检测时应互不相关、互不干扰等。目前数字水印技术的研究已引起广泛关注,但关于多重水印的研究却并不太多。多重水印的应用范围很广泛,如一个数字多媒体作品除了一个或多个原作者的版权标识外,可能还需要添加代理公司、收藏者的版权

标识等。这些不同的版权标识之间要求相互独立,对其中一个标识可以进行单独修改且不会对其他标识造成影响。

在无线通信中,CDMA系统有很多优点,如多址复用、容量大、保密性好、抗干扰能力强等。CDMA技术用给定的伪随机编码调制用户数据,以实现码分多址,按编码分配用户、构造多个完全正交的扩频码对应不同的用户及多个用户可以同时通信。这些特点正好可以满足多重水印的要求。目前已有一些基于CDMA技术的单一水印算法。文献[1]将RGB图像变换到YIQ彩色空间,通过选择Y分量的前15个DCT系数、I分量的前6个DCT系数、Q分量的前3个DCT系数,组成独立的CDMA信道,以嵌入水印信

收稿时间:2007-09-14

基金项目:国家863计划项目(2006AA01Z407)

作者简介:张帆(1967-),男,博士,副教授,主要从事图像处理、模式识别等方面的研究。

息。文献[2]提出了直接在空间域将原始图像分成多层比特平面作为独立CDMA信道的水印嵌入算法。文献[3-4]提出了一种抗裁剪的DWT域CDMA扩频图像水印算法。文献[5]针对压缩和未压缩的视频信号,采用直接序列的CDMA形式的扩频调制方法,在解压的加水印视频信号中恢复水印信息,当二值水印信号加入时,先由一个 m 序列扩展调制为宽带信号。视频帧信号和水印信号可直接在空域叠加或经DCT变换后相加。在多重水印方面,文献[6]提出了一种在数字视频信号中嵌入多重水印的算法,将不同的水印分别嵌入到视频的不同帧中。文献[7]采用线性反馈移位寄存器产生伪随机序列来将多重水印置乱后嵌入宿主图像中。文献[8]利用不同密钥嵌入多重水印。文献[9]提出了一种小波变换域中的多重水印算法。文献[10]提出了一种鸡尾酒水印(Cocktail Watermarking)算法用于图像认证,这种方法可以同时嵌入多个不同性质的水印(鲁棒、脆弱),以实现图像的完整性保护并提高抗攻击性能。

本文提出的基于CDMA水印算法,着眼点在利用CDMA系统多址复用的特点同时嵌入多个水印信息。由于CDMA系统有很好的抗干扰能力并且水印信息在小波变换域中嵌入,所以具有较好的鲁棒性。

1 水印嵌入与检测

水印的嵌入和提取可以视为一次通信过程,水印为信源,图像为信道。水印的嵌入对应于通信中的编码和调制过程,水印的提取对应于通信中的解调过程。

CDMA通信是将相互正交(或准正交)的不同编码分配给不同用户来调制信号,实现多用户同时使用同一频率接入系统和网络的通信,即码分多址通信。实现CDMA的理论基础是扩频通信,即在发送端将待发送的数据用伪随机码进行调制,实现频谱扩展后进行传输,而在接收端则采用相同的伪随机码进行解调及相关处理以恢复原始的数据信息。

本文的水印算法采用双正交小波变换(bi-orthogonal DWT)。在图像处理中经常希望所用滤波器具有线性相位,文献[11]放弃了小波、尺度函数的正交性,给出了构造具有对称性的双正交基的方法,这时对应的滤波器具有线性相位。图像经过小波分解后生成的小波图像具有与空域中不同的特性,表现在图像的能量主要集中在低频部分,即图像的主要部分,也是视觉重要部分。而图像的高频部分,即图像的细节部分则能量较少。在小波变换域中,如果水印信息添加在高频子带中,则水印的

鲁棒性会受到影响。如果水印信息添加在低频子带中,则水印的不可感知性可能会受到影响。在本文方法中,多重水印被嵌入在除HH1以外的其他小波子带中。这些小波子带中的小波系数占全部小波系数的 $3/4$,这个比例会对下面阐述的直接序列扩频中切普速率的选择产生影响。

卷积码是一种信道编码,其实质就是在信息码中增加一定数量的多余码元(称为监督码元),使它们满足一定的约束关系,这样由信息码元和监督码元共同组成一个由信道传输的码字。常把卷积码记为 (n, k, m) 。卷积码将 k 个信息比特编成 n 个比特,码率为 k/n ,纠错性能随 m 的增加而增大,而差错率随 m 的增加而指数下降。通常将 m 称为约束长度。卷积码编码器包括一个由 m 段组成的输入移位寄存器,每段有 k 个,共 $m \times k$ 个寄存器;一组 n 个模2相加器;一个由 n 级组成的输出移位寄存器,对应于每段 k 个比特的输入序列,输出 n 个比特。

本文所用卷积码编码器的码率为 $1/2$ 的 $(2, 1, 2)$ 卷积码,有一位监督位,其约束长度为2,可以在4 b范围内纠正一个错误。在本文方法中,水印为 32×32 的二值图像。如果水印为文字或其他媒体,可以把这些信息扩展或压缩为1 024位的二进制序列,再转化为 32×32 的二值图像。在卷积编码中,二值图像的每行32位作为一组码字输入卷积码编码器,最后形成一个 64×32 的矩阵。

Gold码是由两个码长相等、码时钟速率相同的 m 序列优选对模2加构成的。本文选择长度为 $L=2^9-1=511$ 的Gold码组对水印信息进行正交扩频。先将经过卷积编码和交织编码后的水印信息转换为一维二进制信号 a_k , $k=1, 2, \dots, n$, n 表示要嵌入的水印个数。然后按切普速率 C_r 对 a_k 进行调制,得到调制信号 b_k 。切普速率 C_r 的选择要综合考虑原始图像的尺寸、水印信息量、卷积码编码器的码率以及水印在小波子带中的嵌入情况。为每个水印分配不同的Gold码组 g_k ,与调制信号 b_k 相乘后把各组扩频信号叠加,再经CDMA编码后得欲嵌入的水印信号:

$$w(t) = \sum_{k=1}^n b_k(t) g_k(t) \quad (1)$$

本文利用小波域视觉感知模型改善嵌入在低频子带中水印的不可感知性。文献[12]对小波域图像压缩中量化噪声的感知模型进行了研究,提出了双正交9/7小波变换下的视觉无损(Perceptually Lossless)量化矩阵。量化矩阵由一系列量化因子(Quantization Factor)组成,量化因子是小波分解级数、子带的频率方向以及显示视觉分辨率(DVR)的函数。不同子

带的量化因子的计算公式为:

$$Q_{\lambda,\theta} = \frac{2}{A_{\lambda,\theta}} a 10^{k \left(\frac{\lambda^2 f_0 g_\theta}{r} \right)^2} \quad (2)$$

式中 λ 为小波分解级数; θ 为子带频率方向的索引; r 为显示视觉分辨率; $A_{\lambda,\theta}$ 为各子带基函数的幅值; 其余各项 a 、 k 、 f_0 、 g_θ 为常数。

小波域图像压缩中的量化采用均匀量化(Uniform Quantization)方式,即用各个子带图像中的小波系数除以相应的量化因子 $Q_{\lambda,\theta}$ 并取整,再经过熵编码等方法进行压缩处理。反量化后小波系数的变化范围是 $[-Q_{\lambda,\theta}/2, Q_{\lambda,\theta}/2]$,如果在小波系数上添加不超过上述变化范围的噪声(水印),也可以达到同样的视觉效果。也就是说在设计水印算法时可以把量化因子与水印的嵌入强度联系起来,即 $Q_{\lambda,\theta}$ 给出了在满足水印不可感知条件下小波子带系数所允许嵌入的最大水印幅值。

在本文方法中,水印采用叠加嵌入方式。为了兼顾鲁棒性和不可感知性,在除HH1子带以外的其他小波子带中嵌入最大水印幅值。利用一个二值的伪随机序列(PN)随机地确定水印信息的嵌入位置。PN序列的每一位与嵌入水印的小波系数相对应,如果PN序列中的某一位为0,则与之相对应的小波系数不做任何修改;如果PN序列中的某一位为1,则与之相对应的小波系数按下面的方式进行修改。设 w_1 和 w_2 分别是经CDMA编码后的水印信号序列 w 的最大和最小值, I 和 I' 分别表示嵌入水印前和嵌入水印后的图像,实现水印的嵌入:

$$I'(i, j) = I(i, j) + \frac{w(t)}{w_1 - w_2} Q_{\lambda,\theta} \quad (3)$$

在水印的检测过程中,首先要对嵌水印的图像做双正交小波变换,利用密钥2产生的PN序列和小波域视觉感知模型确定水印的嵌入位置和水印的幅值;然后利用与嵌入水印时相同的Gold码组对扩频水印序列进行解调;再通过解交织和卷积译码得到各个水印信息。

在水印图像经历一些处理、变换或侵权人的恶意攻击后,提取出的水印与嵌入的水印是否完全相同,可以采用提取出的版权信息与原始版权信息之间的相关性来判定版权信息的存在与否。

2 容量分析

数字水印容量是指在宿主图像中嵌入水印的最大信息量。当假定附加噪声为高斯噪声,宿主图像

为传输信源的加性高斯白噪声(AWGN)信道时,则可以利用Shannon公式来估计隐藏信息的容量。本文提出的基于CDMA技术同时嵌入多个水印,其容量会与嵌入单一水印时有所不同。

设噪声服从均值为零,方差为 σ_n^2 的高斯分布。由限平均功率最大熵定理,要求 Y 为高斯分布,设其均值为 m 。在同时嵌入两个水印的情形下,设信道平均输入功率受限: $EW_1'^2 = \sigma_1^2$, $EW_2'^2 = \sigma_2^2$, 且与噪声 N 相互独立,则:

$$EY^2 = \sigma^2 = \sigma_1^2 + \sigma_2^2 + \sigma_n^2 \quad (4)$$

Y 的熵为:

$$H(Y) = - \int_{-\infty}^{\infty} p(y) \lg p(y) dy \quad (5)$$

因 $\int_{-\infty}^{\infty} p(y) dy = 1$, $\int_{-\infty}^{\infty} (y-m)^2 p(y) dy = \sigma^2$, 所以:

$$H(Y) = \frac{1}{2} \lg 2\pi e(\sigma_1^2 + \sigma_2^2 + \sigma_n^2) \quad (6)$$

类似地:

$$H(Y | W_2') = \frac{1}{2} \lg 2\pi e(\sigma_1^2 + \sigma_n^2) \quad (7)$$

$$H(Y | W_1') = \frac{1}{2} \lg 2\pi e(\sigma_2^2 + \sigma_n^2) \quad (8)$$

$$H(Y | W_1' W_2') = \frac{1}{2} \lg 2\pi e\sigma_n^2 \quad (9)$$

则容量表示为:

$$C_1 = \max_{p(w_1')p(w_2')} I(W_1'; Y | W_2') = \max_{p(w_1')p(w_2')} [H(Y | W_2') - H(Y | W_1' W_2')] = \frac{1}{2} \lg \left(1 + \frac{\sigma_1^2}{\sigma_n^2} \right) \quad (10)$$

$$C_2 = \frac{1}{2} \lg \left(1 + \frac{\sigma_2^2}{\sigma_n^2} \right) \quad (11)$$

$$C_{12} = \frac{1}{2} \lg \left(1 + \frac{\sigma_1^2 + \sigma_2^2}{\sigma_n^2} \right) \quad (12)$$

所以,嵌入两个水印时,其容量不是嵌入相应单一水印时容量的简单叠加。当嵌入的水印 W_1' 和 W_2' 相互独立时,其容量 C_1 、 C_2 与 C_{12} 之间存在下列关系:

$$\max[C_1, C_2] \leq C_{12} \leq C_1 + C_2 \quad (13)$$

即嵌入两个水印时,其容量大于任何一个单一水印的容量,但小于两个单一水印容量之和。上面的结果不难推广到嵌入多个水印时的情况。

3 实验结果

本文采用512×512的Lena、Baboon、Fishingboat、

Peppers、Couple和Girl等灰度图像，对两幅水印为 32×32 的二值图像进行了实验。

本文在一些常见的图像处理操作和攻击情况下(如JPEG压缩、高斯噪声和中值滤波等)，对嵌入信息的鲁棒性进行了实验，误码率性能的实验结果如表1所示。图1是在高斯噪声攻击条件下峰值信噪比与误比特率之间的关系。

表1 误码率性能

	JPEG $Q=50$	JPEG $Q=30$	Gaussian Noises ($\sigma^2=1$)	Gaussian Noises ($\sigma^2=4$)	Median Filtering (4×4)
PSNR/dB	31.72	28.49	29.32	25.47	24.32
BER/(%)	0	2.51	1.67	7.62	12.38

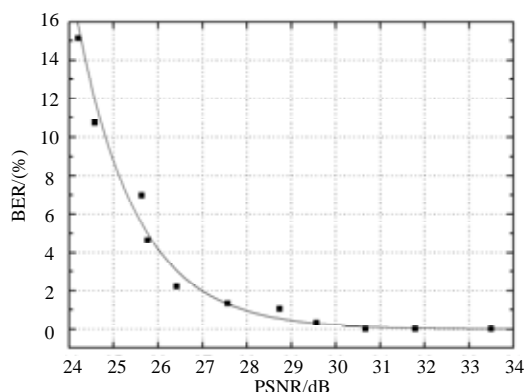


图1 高斯噪声攻击条件下峰值信噪比与误比特率之间关系

由于不同文献采用的实验方法和参数有所不同，所以在不同方法的实验结果之间进行精确的比较是困难的，但是可以做出大致的比较。与文献[1-5]相比，由于本文方法嵌入的信息量比较大，而且嵌入的幅值也比较大，所以在峰值信噪比方面比上述文献的要低一些。如文献[3-4]的实验结果中，嵌入水印信息后，图像的PSNR达 $40 \sim 45$ dB，文献[5]嵌入水印图像的PSNR为 $38 \sim 40$ dB，本文方法中PSNR为 35 dB左右。在误比特率方面，由于本文采用了卷积编码和交织编码等方法，性能有所提高。在嵌入信息小于本文方法的情况下，在JPEG压缩因子为 50 时，文献[2]方法的BER为 $5\% \sim 25\%$ ，文献[3-4]方法的BER为 $0\% \sim 0.2\%$ ，文献[5]方法的BER为 $0.5\% \sim 2\%$ ，而本文方法的BER为 0 。

4 结 论

本文提出了一种基于CDMA的多重水印算法，利用CDMA系统多址复用的特点，在小波变换域中同时嵌入多个水印。检测时不需要原始图像。采用

信道编码和小波域视觉感知模型改善水印信息的检测可靠性和不可感知性。由于CDMA系统有很好的抗干扰能力并且水印信息在小波变换域中嵌入，所以水印具有较好的鲁棒性。本文对基于CDMA的多重水印的容量问题进行了分析。当嵌入两个水印时，其容量大于任何一个单一水印的容量，但小于两个单一水印容量之和。

参 考 文 献

- [1] KOHDA T, OOKUBO Y, SHINOKURA K. Digital watermarking through CDMA channels using spread spectrum techniques[C]//In Proceedings of IEEE 6th International Symposium on Spread Spectrum Techniques and Applications. Parsippany: IEEE Press, 2000: 671-674.
- [2] VASSAUX B, BAS P, CHASSERY J. A new CDMA technique for digital image watermarking enhancing capacity of insertion and robustness[C]//In Proceedings of 2001 IEEE International Conference on Image Processing. Thessalonica, Greece: IEEE Press, 2001: 983-986.
- [3] FANG Yan-mei, WU Shao-quan, HUANG Ji-wu. DWT-Based CDMA watermarking resist cropping[J]. ACTA Automatica Sinica, 2004, 30(3): 442-448.
- [4] FANG Yan-mei, HUANG Ji-wu, SHI Yun-qing. Image Watermarking Algorithm Applying CDMA[C]//In Proceedings of the 2003 International Symposium on Circuits and Systems. Bangkok, Thailand: IEEE Press, 2003: 948-951.
- [5] HARTUNG F, GIROD B. Watermarking of uncompressed and compressed video[J]. Signal Processing, 1998, 66: 283-301.
- [6] COX I, KILIAN J, SHAMOON T. Secure spectrum watermarking for multimedia[J]. IEEE Transactions on Image Processing, 1997, 6: 1673-1687.
- [7] HSU C, WU Ja-ling. Hidden digital watermarks in images[J]. IEEE Transactions on Image Processing, 1999, 8(1): 58-68.
- [8] WONG P, AU O, YEUNG Y. A novel blind multiple watermarking techniques for images[J]. IEEE Transactions on Circuits and Systems, 2003, 13(8): 813-830.
- [9] RAVAL M, PRITI P. Discrete wavelet transform based multiple watermarking schemes[C]//In Proceedings of 2003 Conference on Convergent Technologies for Asia-Pacific Region. New Delhi, India: Allied Publishers Ltd, 2003: 935-938.
- [10] LU C, LIAO H. Multipurpose watermarking for image authentication and protection[J]. IEEE Transactions on Image Processing, 2001, 10(10): 1579-1592.
- [11] COHEN A, DAUBECHIES I. Bi-orthogonal bases of compactly supported wavelets[J]. Communications on Pure and Applied Mathematics, 1992, 45(7): 485-560.
- [12] WATSON A, YANG G. Visibility of wavelet quantization noise[J]. IEEE Transactions on Image Processing, 1997, 6(8): 1164-1174.