

基于多小波变换的 CDMA 数字水印研究^{*}

朱 岩^{1,2}, 冯登国², 杨永田¹

(1. 哈尔滨工程大学 计算机科学与技术学院, 黑龙江 哈尔滨 150001;

2. 中国科学院 信息安全国家重点实验室, 北京 100039)

摘 要: 在多小波变换和图像多小波视觉掩蔽模型基础上, 在保证水印鲁棒性的前提下, 为达到增大水印容量的目的, 提出了一种新颖的基于多小波变换的码分多址 (CDMA) 数字水印方案。试验结果表明, 所提出的算法是既具有较高的嵌入容量, 又具有较强的鲁棒性。

关键词: 数字水印; 扩频; 码分多址; 多小波变换

中图分类号: TP391 **文献标识码:** A **文章编号:** 0529-6579 (2004) S2-0180-04

数字水印是一种将信息隐藏于数字多媒体中的通信技术, 在 Costa 的脏纸模型^[1]中, 码书编码由嵌入信息分布和参考源对编码方式的影响来确定, 其中, 参考源的统计特征是一个重要因素, 一方面, 期望它的统计特征能服从某种已知分布; 另一方面, 期望编码形式能充分利用参考源信息。基于这两方面要求, 本文在多小波变换下, 利用图像多小波分解的高频子带近似服从高斯分布的特点以及视觉掩蔽模型构造出一种新颖的自适应水印方案。多小波变换是在小波变换基础上发展起来的, 除了具有小波变换多分辨率逼近、快速算法等性质以外, 还有短支撑、高消失矩、同时达到对称和正交性的特点, 为了充分地利用这些优点, 本文采用分解预处理、边界处理、图像整形等技术来达到图像多小波变换正交、低复杂性和紧凑的输入图像表示的性质。

扩频是目前主要采用的一种水印技术, Cox 等^[2]提出了将水印信息用伪随机数列进行扩展, 并隐藏于载体感知重要成分之中的扩频水印思想。一般将其应用到各种变换域中, 如离散余弦 (DCT)、小波变换等。扩频水印具有鲁棒性强、高度保密的特点, 但是有水印容量低的缺点, 为了改善性能, 将码分多址技术 (CDMA) 与扩频技术相结合来增加通信容量。大量的研究表明, 利用 CDMA 原理在数字媒体中嵌入数字水印信息是一种行之有效的方法。Vassaux 等^[3]提出直接在空间域将原始图像分成多层比特平面作为独立 CDMA 信道水印嵌入技术。基于多小波和 CDMA 两种技术, 本文提出了一种基于多小波变换的 CDMA 水印算法, 既保留了鲁

棒性、保密性的优点, 又具有较大的容量。

1 多小波理论

1.1 多小波及多小波变换

通常标量小波有一个尺度函数 $\phi(x)$ 和小波函数 $y(x)$, 而多小波变换^[4] 有多个尺度函数和小波函数, 分别称为多尺度函数和多小波函数, 通常使用多维向量函数进行表示。令

$$\Phi(x) = [\phi_1(x) \phi_2(x) \cdots \phi_r(x)]^T (r \in N)$$

表示多分辨率分析空间 $\{V_k\}_{k \in \mathbb{Z}}$ 上的 r -维多尺度函数, 与其对应的多小波函数

$$\Psi(x) = [y_1(x) y_2(x) \cdots y_r(x)]^T$$

构成了正交互补子空间上 $\{W_k\}$ 的正交基, 即 W_j 是 V_j 在 V_{j+1} 中的正交补空间。 $\Phi(x)$ 和 $\Psi(x)$ 满足

$$\begin{aligned} \Phi(x) &= \sqrt{2} \sum_{k \in \mathbb{Z}} H_k \Phi(2x - k) \\ \Psi(x) &= \sqrt{2} \sum_{k \in \mathbb{Z}} G_k \Phi(2x - k) \end{aligned} \quad (1)$$

其中, $\{H_k\}$ 和 $\{G_k\}$ 是 $r \times r$ 矩阵滤波器。

多小波变换与小波变换相比更具一般性, 首先, 滤波器系数 H_k 是矩阵而不是标量; 其次, 可以方便地构造尺度因子 m 大于 2 的多小波。这些差异能够带来更优越的属性, 例如短紧支、正交、对称、更高消失矩等, 应用多小波变换的关键就在于如何更好的利用这些额外的自由度。目前研究较多的是 DGHM 多小波, 它既保持了标量小波所具有的良好时域和频域局部化特征, 又具有紧支性、二阶逼近、多尺度函数对称性、多小波函数分别具有对称和反对称性、尺度函数的整数平移相互正交等显著

^{*} 收稿日期: 2004-08-28

作者简介: 朱岩 (1974 年生), 男, 博士研究生; E-mail: martinzh@msn.com

特点, 本文也将在 DGHM 多小波基础上进行研究。

1.2 多小波的预处理

多小波预处理是指从一个给定标量数据流生成 r 维矢量输入流的处理过程。通常是通过构造滤波器 Q 来实现, 滤波器长度、逼近阶数、频率响应和对称性是几个需考虑的因素, 其中逼近阶数影响多小波分解的逼近程度和重构后信号误差大小, 是一个较为重要的因素。设函数 f 在多小波多分辨率分析空间 V_n 上的投影 $P_n f$ 表示 f 在分辨率 m^{-n} 上的逼近, 称多尺度函数 ϕ 具有逼近阶 p , 如果满足

$$\|f(x) - P_n f(x)\| = O(m^{-np})$$

其中, f 有 p 阶连续导数, 显然, p 越大逼近程度越高, 误差越小。设 f 是多小波尺度函数空间上的连续函数, 对多尺度函数 $\phi, f(x)$ 可由多尺度函数的线性组合表示:

$$f(x) = \sum_n (v_{1,n} \phi_1(x-n) + v_{2,n} \phi_2(x-n)) \quad (2)$$

令采样序列 $s(n)$ 为函数 $f(x)$ 在整数点和半整数点上的采样值:

$$s(2n) = f(n), s(2n+1) = f(n+1/2) \quad (3)$$

对于 DGHM 多尺度函数, 在整数和半整数的非零函数值仅有 $\phi_1(1/2), \phi_2(1/2), \phi_2(1), \phi_2(3/2)$, 可得:

$$\begin{aligned} s(2n) &= v_{2,n-1} \phi_2(1) \\ s(2n+1) &= v_{1,n} \phi_1(1/2) + \\ &\quad v_{2,n} \phi_2(1/2) + v_{2,n-1} \phi_2(3/2) \end{aligned} \quad (4)$$

不难解得:

$$\begin{aligned} v_{1,n} &= \frac{\phi_2(1) s(2n+1) - \phi_2(1/2) s(2n+2)}{(\phi_2(1) \phi_1(1/2))} - \\ &\quad \frac{\phi_2(3/2) s(2n)}{(\phi_2(1) \phi_1(1/2))} \\ v_{2,n} &= s(2n+2) / \phi_2(1) \end{aligned} \quad (5)$$

由此构造的预滤波器组保留了 DGHM 的阶数, 同时它与对称扩展法自然地相协调, 即在信号边界对称地扩展有限长信号, 那么经过预处理输出的两列将是近似对称的。

1.3 多小波分解结构

在标量小波的单层分解中, 二维数据被低通滤波器 L、高通滤波器 H 分解为表示不同方向的 4 个子带, 而多小波变换使用两个滤波通道, 将 2 个低频、高频滤波器分别表示为 L_1, L_2, H_1, H_2 , 因此, 多小波变换生成 16 个子带, 行方向的第 2 高通滤波和列的第 1 低通滤波的子带可表示 $L_1 H_2$, 单层图像分解的标量小波和多小波比较见图 1。

对于多层多小波分解, 在上一层分解的基础

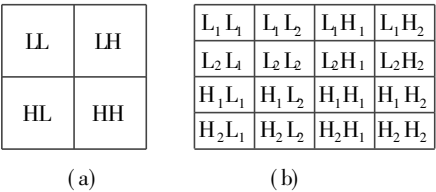


图 1 在一层标量多小波 (a) 和多小波分解后的图像子带 (b)

Fig 1 Image subbands after a single-level decomposition for scalar wavelets (a) and multiwavelets (b)

上, 将低频子带 $L_i L_j (i, j \in \{1, 2\})$ 继续进行分解。首先对原始图像在行方向进行预处理, 再对列方向进行预处理, 然后分别在行和列 2 个方向进行多小波变换得到一层分解后的图像, 对于 n 层多小波变换, 则继续对低频子带进行变换, 无需进行预处理, 直到 n 层变换结束。

2 基于多小波的数字水印

2.1 视觉掩蔽模型

由于小波系数的多样性, 在 DMWT 下还没有统一的视觉模型, 已有的模型都是与具体的小波变换相关的。本文根据视觉的对比度和掩蔽效应^[5], 提出一种基于多小波变换的视觉掩蔽模型。在特定的分解层 l 和方向 θ 中的坐标 (x, y) 处的小波分解系数的水印增益可表示为

$$g^{l,\theta}(x,y) = \beta_{x,y} \sqrt{k_{l,\theta}^2 |x(x,y)|^2 + C_{l,\theta}^2} \quad (6)$$

其中, $x(x,y)$ 表示在特定子带的 DMWT 分解系数以 (x,y) 为中心的临近区域内用低通滤波器滤波后得到的幅值, 一般采用 3×3 低通滤波矩阵进行滤波, 根据亮度掩蔽效应, 背景亮度变化而产生的增益变化由参数 β 表示, 计算公式为

$$\beta_{x,y} = 3.62(|x_{dc}(x,y) - 0.59|)^2 + 0.68 \quad (7)$$

其中, $x_{dc}(x,y)$ 是坐标 (x,y) 在最低层 DWT 低通子带对应像素点的幅值模, $k_{l,\theta}$ 和 $C_{l,\theta}$ 为子带相关常数 (见表 1), 表中 k_0 取值依靠图像进行选择, 范围在 0.5~1.0, 一般情况下, 使用缺省值 0.9。

表 1 多小波变换下视觉掩蔽模型常数表

Tab 1 Table of constants used in the DMWT marking model

Layer	HL/LH		HH	
	k	C	k	C
1	0.16 k_0	2.8	0.15 k_0	4.8
2	0.29 k_0	1.5	0.30 k_0	1.9
3	0.35 k_0	2.1	0.33 k_0	2.0

2.2 数字水印算法

根据扩频以及 CDMA 技术, 提出了一种基于视

觉感知模型的数字水印方案，其嵌入过程如下：

步骤 1：水印建立和预处理。原始灰度图像 S 经行列方向的预处理后，进行 L 层多小波分解，最后在图像整形处理后得到载体图像 C_s 。再将 C_s 按照分解层 $l \in \{1, \dots, L\}$ 和方向 $\theta = \{HL, LH, HH\}$ 分成几个嵌入块 $C_s^{l,\theta}$ 。令分解层 l 和方向 θ 的块中嵌入的信息数量为 m bit，将信息表示为二进制的形式并通过映射转换成矢量 $b^{l,\theta} = \{b_1^{l,\theta}, b_2^{l,\theta}, \dots, b_m^{l,\theta}, b_i^{l,\theta} \in \{-1, 1\}\}$ 。按照水印密钥 Key，伪随机数生成器构造 m 个伪随机序列

$$w_i = \{w_i(1), w_i(2), \dots, w_i(N)\}, \\ w_i(k) \in [0, 1], (i = 1, \dots, m)$$

可以使用 CDMA 中的正交扩频码，如 Gold 码、 m 序列或 Kasami 码等，经 $[0, 1]$ 区间缩放来获得。根据 CDMA 技术，在分解层 l 和方向 θ 的块中，嵌入的水印序列可表示为

$$W^{l,\theta}(n) \sum_{i=1}^m b_i^{l,\theta} w_i(n), n = 1, \dots, N \quad (8)$$

其中， $N \in \mathbb{Y}$ 是每块中的序列长度。水印密钥即用于嵌入信息的加密，又用于扩频序列的生成。

步骤 2：水印嵌入过程

由于图像多小波分解后的逼近系数表征图像中的低频部分，对它的任何改动将影响图像的质量，因此，水印嵌入在图像的细节系数中实现。首先，根据本文提出的视觉掩蔽模型，计算出图像多小波变换后细节系数的感知增益 $g^{l,\theta}$ ；然后，在分解层 l 和方向 θ 的细节系数块 $C_w^{l,\theta}$ 中，水印序列 $W^{l,\theta}$ 的嵌入过程可以表示为

$$C_w^{l,\theta}(n) = C_s^{l,\theta}(n) + \alpha g^{l,\theta}(n) W^{l,\theta}(n) \quad (9)$$

其中， $C_w^{l,\theta}$ 是嵌入水印后的图像，且 $x, y \in \mathbb{Y}$ ， α 为嵌入强度，对 m bit 嵌入则强度要缩小 $1/\sqrt{m}$ 。

步骤 3：含水印图像生成

在各块嵌入水印后须将各块重新组合，经过图像整形的逆变换、多小波反变换和行列方向的后处理之后，得到最终的水印图像 S' 。

水印信息提取采用相关检测的盲水印方案，提取过程如下：与水印的嵌入过程类似，对待检测的图像 S'' 经行列方向的预处理后，进行 L 层多小波分解，最后在图像整形处理后得到载体图像 C''_s 。并将 C_s 按照分解层 $l \in \{1, \dots, L\}$ 和方向 $\theta = \{HL, LH, HH\}$ 分成几个嵌入块 $C_s^{l,\theta}$ 。同时，按照水印密钥 Key，使用伪随机数生成器构造 m 个伪随机序列

$$w_i = \{w_i(1), w_i(2), \dots, w_i(N)\}, \\ w_i(k) \in [0, 1], \quad i = 1, \dots, m$$

根据正交序列的互相关函数特性，在分解层 l 和方向 θ 第 i bit 的水印信息可由如下判断公式得到

$$b_i^{l,\theta} = \begin{cases} 1 & r_i^{l,\theta} \geq \tau \\ -1 & r_i^{l,\theta} \leq -\tau \end{cases} \quad (10)$$

其中， τ 是检测阈值， $r_i^{l,\theta}$ 是图像和水印的相关：

$$r_i^{l,\theta} = \sum_{n=1}^N C_s^{l,\theta}(n) w_i(n), i = 1, \dots, m \quad (11)$$

最终，将提取信息解密即可得到嵌入的原始信息。

3 试验与分析

本试验以“Lena”灰度图像为测试图，多小波进行两层分解，采用本文所提出 CDMA 水印算法，两层多小波分解的嵌入块的系数个数不同，第 1 层分解系数比第 2 层多 4 倍，因此将第 2 层的嵌入量减少 4 倍。试验过程分解图例如图 2 所示。

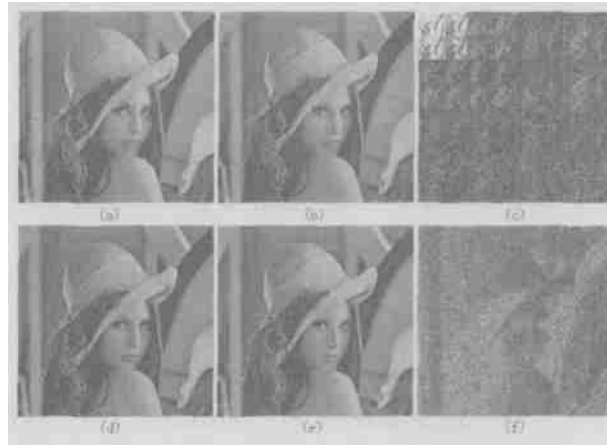


图 2 水印嵌入的处理过程
Fig. 2 The processes of watermarking embedding

试验所用的正交扩频码是由伪随机数生成器产生的正态分布序列 $w_i: N(0, 1)$ ，并设嵌入信息 $b_i (i = 1, \dots, m)$ 的取值是随机分布的。根据中心极限定理，当 m 足够大时，序列 W 的统计分布应服从正态分布 $W: N(0, m)$ 。为了检验在嵌入算法步骤 1 中 CDMA 正交扩频码的性能，对 128 bit 嵌入而形成的扩频序列进行统计分析（图 3）。

在图 3 中左图是实验数据的分布情况，并使用拟合软件进行分析，图中曲线为拟合结果，右图是拟合的计算结果，可以看出，分布为 $N(0.01, 11.31^2)$ ，这与理论值 $N(0, 11.31^2)$ 是一致的。

为了检验算法鲁棒性，采用 JPEG 压缩进行试验，压缩算法是 Matlab 中的压缩算法，强度在 10%~100% 之间。在保证不可感知的前提下，对 480 bit 信息嵌入（第 1 层为 3×128 bit，第 2 层为 3×32 bit）的试验结果见图 4 (a) 所示，可以看出

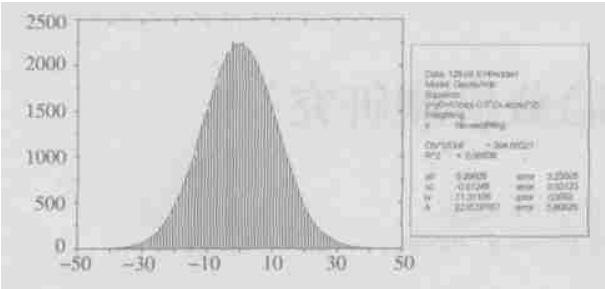


图 3 128-bit CDMA 序列分布图及正态拟合参数估计结果

Fig 3 The distribution histogram of 128-bit CDMA sequence and the result of parameter estimates for normal fit

本算法具有很强的抵抗 JPEG 压缩能力，在压缩率达到 35% 仍然有很好的性能。同时，图中给出了第 1 层和第 2 层的鲁棒性对比，可知第 2 层结果要好于第 1 层。为了检验算法的容量和鲁棒性之间的关系，分别嵌入 240、480、960 bit 的负载，并在 JPEG 压缩下观察其比特错误率的变化情况。从图 4 不难看出，随着负载增加，鲁棒性能下降，特别是在压缩 50% 情况下算法依然有很好性能。

4 结 论

本文结合多小波变换的优点以及扩频水印具有鲁棒性强的特点，在视觉掩蔽模型基础上，提出了一种新颖的基于多小波变换的 CDMA 数字水印方案。通过较全面的实验分析表明所提出的算法是既具有较高的嵌入容量，又具较强鲁棒性。

参考文献:

[1] COHEN A S, LAPIDOTH A. Generalized writing on dirty paper[J] . In Proc of ISIT, 2002: 227.
[2] COX I J, KILIAN J, SHAMOON T, et al. Secure spread spectrum watermarking for multimedia[J] . IEEE Trans on Image Processing, 1997, 6: 1673—1687.

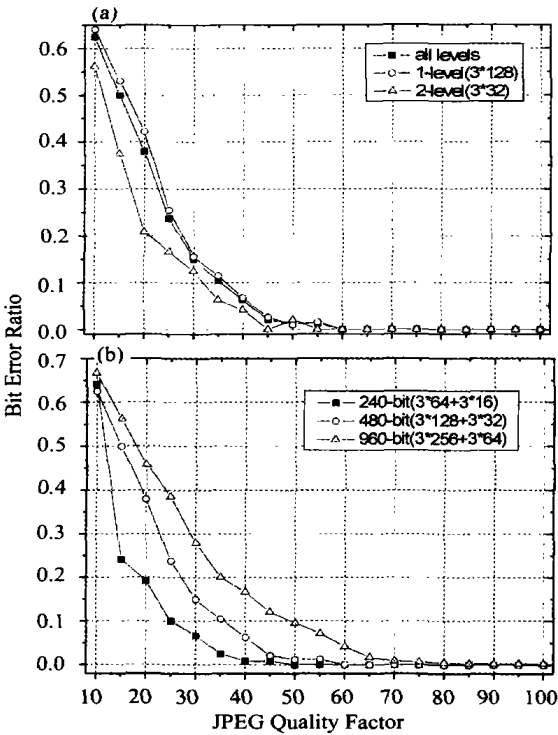


图 4 (a) 480 bit 和 (b) 240、480、960 bit 在 2 层水印嵌入时 JPEG 压缩下的 BER 变化

Fig 4 The variation of BER under JPEG compression for (a) 480 bit (b) 240, 480, 960 bit and 2-levels embedding

[3] VASSAUX B, BAS P, CHASSERY J M. A new CDMA technique for digital image watermarking enhancing capacity of insertion and robustness[J] . Proc of IEEE Int Conf on Image Processing, Thessalonica, Greece, 2001, 3: 983—986.
[4] THAM J Y, SHEN L X, LEE S L, et al. A general approach for analysis and application of discrete multiwavelet transforms [J] . IEEE Trans on Signal Processing, 2000, 48: 457—464.
[5] MAYACHE A, EUDE T, CHERIFI H. A comparison of image quality models and metrics based on human visual sensitivity [C] . Proc of International Conf on Image Proc (ICIP '98), 1998, III: 409—413.

Research on CDMA Digital Watermarking Based on Multiwavelet Transform

ZHU Yan^{1,2}, FENG Deng guo², YANG Yong tian¹

(1.Computer Science and Technology School, Harbin Engineering University, Harbin 150001, China;
2.The State Key Laboratory of Information Security, The Chinese Academy of Sciences, Beijing 100039, China)

Abstract: In terms of multiwavelet translation and vision marking model in image multiwavelet transform domain, this paper presents a novel code division multiple access (CDMA) watermarking scheme based on multiwavelet translation to maximize watermark capacity under the precondition of robustness. The experiment results demonstrate that the proposed algorithm provides the higher embedding capacity as well as the more robust against attack.

Key words: digital watermarking; spread spectrum; code division multiple access; multiwavelet