

扩频 CDMA 水印性能分析及其多小波域内的应用研究

朱 岩^{1),2)} 孙中伟²⁾ 杨永田¹⁾ 冯登国²⁾

¹⁾(哈尔滨工程大学计算机科学与技术学院 哈尔滨 150001)

²⁾(中国科学院研究生院信息安全国家重点实验室 北京 100049)

摘 要 通过对扩频码分多址(CDMA)水印模型的编码及检测方法进行理论分析,阐述了信息嵌入量、扩频码长、检测错误率等指标之间存在的制约关系,并使用实验进行比较和验证.在理论分析的基础上,依据多小波分解系数优良统计分布特征和图像多小波视觉掩蔽模型,提出了一种新颖的基于多小波变换的扩频 CDMA 数字水印方案.理论结果与实验数据对比表明所提出的模型和算法既有较高的嵌入容量,又具有较强的鲁棒性和安全性.

关键词 数字水印;扩频水印;CDMA;多小波变换;视觉掩蔽模型

中图法分类号 TP391

Performance Analysis of Spread Spectrum CDMA Watermarking and Applied Research in Multiwavelet Domain

ZHU Yan^{1),2)} SUN Zhong-Wei²⁾ YANG Yong-Tian¹⁾ FENG Deng-Guo²⁾

¹⁾(Computer Science and Technology School, Harbin Engineering University, Harbin 150001)

²⁾(State Key Laboratory of Information Security, Graduate School of the Chinese Academy of Sciences, Beijing 100049)

Abstract By means of the theory analysis of encoding and detection methods in spread spectrum Code Division Multiple Access (CDMA) watermarking model, this paper illuminates the correlations among embedded information number, spreading code length and detection error probability, and these conclusions are compared and verified with experimentations. Furthermore, taking advantage of well-defined statistical distribution of multiwavelet coefficients and visual masking model in image multiwavelet domain, this paper presents a novel spread spectrum CDMA watermarking scheme based on multiwavelet transform. Comparing the theoretical results with the empirical data obtained by experimentation, the research demonstrates that the proposed model and algorithm provide higher embedding capacity, as well as more robust and secure against attacks.

Keywords digital watermarking; spread spectrum watermarking; CDMA; multiwavelet transform; visual masking model

1 引 言

数字水印是隐蔽通信和知识产权保护的一种重要方法,目前广泛采用的数字水印技术是扩频(spread spectrum)技术,Cox 等人^[1]最早提出了扩频

水印的思想,即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份之中.扩频水印具有鲁棒性强、高度保密的特点,但是也有水印容量低的缺点.在通信系统中,码分多址 CDMA (Code Division Multiple Access) 是一种有效的通信方式,CDMA 系统有诸多优点,如可多址复用、保密性好、容量大、

抗干扰力强、抗噪声等。因此,将 CDMA 技术与扩频水印技术相结合是一种行之有效的水印构造方法,既可以保证数字水印的鲁棒性和安全性,又可以提高信道容量。大量的研究已经表明,利用 CDMA 技术在数字媒体中嵌入信息是一种实用、有效的方法,如 Vassaux 等^[2]提出在空间域将原始图像分成多层嵌入平面作为独立 CDMA 信道的水印技术并验证了算法健壮性;文献^[3]描述了扩频 CDMA 技术在 DCT 变换域内的水印方案。

为了系统地阐明数字水印的原理和性能,很多学者在建立水印的数学模型基础上从理论上给予了分析和研究^[4~8],例如针对一般扩频水印模型, Hernández 等人采用信号检测理论进行了大量细致的研究^[5,6];对于量化索引模型(quantization index modulation),Chen 等人在提出模型的基础上,使用脏纸(dirty paper)理论进行的性能分析^[7,8]等。然而,目前对扩频 CDMA 水印研究多是采用实验来评估算法性能及选择参数,缺乏理论上的分析和研究,本文通过建立扩频 CDMA 水印数学模型,根据信号统计和检测理论,提出一种带有匹配滤波的相关检测器,并在理论上较系统地分析了扩频 CDMA 数字水印模型的性能,包括信息嵌入量与图像失真程度、扩频序列长度、相关检测系数的关系以及水印模型的检测错误率和水印容量等,并结合实验进行比较和验证。

本文在分析水印模型的基础上,提出改进水印方案的两个重要因素:(1)参考源的统计特征能否服从某种已知分布;(2)能否充分利用参考源信息来嵌入水印。为了实现这两个因素,首先,需要选择适当的嵌入域,使它满足较好的统计特征;同时需要实现嵌入域内的感知模型,来最大化地应用参考源信息。本文基于这两方面的要求,在多小波变换下,利用图像多小波分解后高频子带系数具有较好的近似高斯分布的特点以及构造基于多小波的视觉掩蔽模型来达到水印自适应嵌入的目的,提出了一种新颖的基于多小波变换的扩频 CDMA 数字水印方案。多小波变换在图像处理方面虽然具有短紧支、正交、对称、高消失矩等优点^[9,10],但也有结构复杂、需要矢量化过程、不易实现等缺点。本文通过采用分解预处理、边界处理、图像整形、后期处理等技术,实现了图像多小波变换的正交、低复杂性和紧凑图像表示的性质。最后,通过大量实验结果表明,本文所提出的算法有图像失真小、鲁棒性强、容量大、安全性高的特点,特别是在高 JPEG 压缩下仍然具有很好的健壮性。

本文第 2 节给出扩频 CDMA 水印模型并从理

论和实验两方面分析模型性能;第 3 节在多小波变换基础上,结合扩频 CDMA 水印模型推荐了一种新颖的数字水印方案;实验结果和分析在第 4 节中进行说明;最后总结全文。

2 基于 CDMA 的扩频数字水印

本节通过建立扩频 CDMA 水印数学模型,根据信号统计和检测理论对水印模型的性能进行较全面的分析,包括信息嵌入量与图像失真程度、扩频序列长度、相关检测系数的关系以及检测错误率和水印容量等,并结合实验给予比较和验证。

2.1 扩频 CDMA 数字水印模型

原始灰度图像 S 经变换和预处理后得到载体图像 $X = \{x_0, x_1, \dots, x_{N-1}\}$, 设嵌入信息数量为 L 比特,将信息表示为二进制的形式并通过映射转换成矢量 $B = \{b_0, b_1, \dots, b_{L-1}\}$, $b_i \in \{-1, 1\}$ 。按照水印密钥 Key ,使用伪随机数生成器构造 L 个伪随机序列 $w_i = \{w_{i,0}, w_{i,1}, \dots, w_{i,N-1}\}$ ($i=0, 1, \dots, L-1$), w_i 服从正态分布,序列的生成可以使用 CDMA 中的正交扩频码,如 Walsh 码、Gold 码、 m 序列或 Kasami 码等经 $[0, 1]$ 区间缩放来获得。根据 CDMA 技术,水印嵌入的编码序列 $W = \{W_0, W_1, \dots, W_{N-1}\}$ 中的每个元素可表示为

$$W_i = \sum_{l=0}^{L-1} b_l w_{l,i}, \quad i=0, 1, \dots, N-1 \quad (1)$$

其中, $N \in \mathbb{N}$ 是扩频序列长度。水印密钥 Key 即用于嵌入信息的加密,又用于扩频序列的生成,决定了水印算法的安全性。设对载体信号 x_i 由图像感知模型计算得到的水印权重因子为 g_i , 则嵌入 L 位信息的公式可表示为

$$y_i = x_i + g_i W_i = x_i + g_i \sum_{l=0}^{L-1} b_l w_{l,i} \quad (2)$$

其中, $i=0, 1, \dots, N-1$ 。计算所得含有水印信号 $Y = \{y_0, y_1, \dots, y_{N-1}\}$ 再经过信号反变换得到含有水印的图像 S' 。

由 Walsh 码以及 m 序列等改进的正交扩频码均具有正交的特性,互相关函数为零,因此不同码间的多址干扰为零。设伪随机序列 w_i 服从均值为零的正态分布,即 $w_i \sim N(0, \sigma_w^2)$, 且序列之间相互独立、正交,根据正交扩频序列相关函数的特性,不妨假设任意两个扩频序列满足

$$E\left(\frac{1}{N} \sum_{i=0}^{N-1} w_{j,i} w_{l,i}\right) = \begin{cases} \sigma_w^2, & j=l \\ 0, & \text{其它} \end{cases} \quad (3)$$

根据正态分布性质和中心极限定理,式(1)中 W_i 满

足高斯正态分布

$$W_i \sim N(0, L\sigma_w^2) \quad (4)$$

即在扩频序列长度 N 不变的情况下, 图像的失真 δ 与嵌入信息数量的平方根 \sqrt{L} 成正比. 虽然 L 越大嵌入信息越多, 但是图像失真也越严重.

通过实验来验证嵌入量与失真关系和 CDMA 正交扩频码的性能, 实验所用的正交扩频码是由 Walsh 码伪随机数生成器产生的正态分布序列 $w_i \sim$

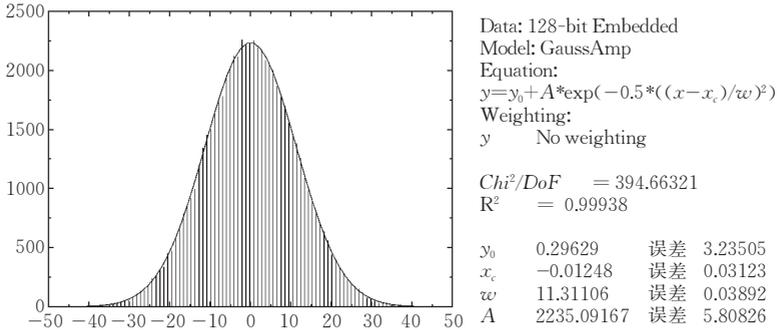


图 1 128bit CDMA 扩频序列统计分布图及正态拟合参数估计结果

2.2 扩频 CDMA 水印检测器设计

我们知道时域图像本身的分布并不服从某种特定的分布, 但是图像在变换域内却能表现出很好的分布特征, 根据这种特点, 假设信道噪声和载体作品在变换域下服从均值为 0 的高斯分布. 在式 (2) 中,

设 $x'_i = x_i + g_i \sum_{l=0, l \neq i}^{L-1} b_l w_{l,i}$, 根据高斯分布独立、正交的性质, 由式 (3) 可知 x'_i 服从均值为零的高斯分布, 不妨令 $x'_i \sim N(0, \sigma^2)$, 则对水印嵌入信息 b_j 而言, 载

有水印的信号可表示为 $y_i = x'_i + g_i b_j w_{j,i}$. 更为一般地, 将水印检测问题看作在两种假设 H_{-1} 和 H_1 中的参数检验问题, 其中 H_1 表示存在信息 $b_j = 1$, H_{-1} 表示存在比特信息 $b_j = -1$, 因此水印检测过程可表示为如下的多样本二元假设检验:

$$\begin{cases} H_1: y_i = x'_i + g_i w_{j,i}, & i=0, 1, \dots, N-1 \\ H_{-1}: y_i = x'_i - g_i w_{j,i} \end{cases} \quad (5)$$

由于嵌入水印是一种弱信号, 则在 H_1 假设下, y_i 的概率密度为 $p_y(y_i | H_1) = p_{x'}(y_i - g_i w_{j,i})$; 而在 H_{-1} 假设下, y_i 的概率密度 $p_y(y_i | H_{-1}) = p_{x'}(y_i + g_i w_{j,i})$. 如果图像变换域内的变换系数统计独立, 那么 N 维样本矢量的概率密度是单样本概率密度的乘积, 于是 H_{-1} 和 H_1 两种假设下的联合概率密度分别为

$$p_Y(Y | H_1) = \prod_{i=0}^{N-1} \frac{1}{\sqrt{2\pi\sigma}} \exp\left(-\frac{(y_i - g_i w_{j,i})^2}{2\sigma^2}\right)$$

$$p_Y(Y | H_{-1}) = \prod_{i=0}^{N-1} \frac{1}{\sqrt{2\pi\sigma}} \exp\left(-\frac{(y_i + g_i w_{j,i})^2}{2\sigma^2}\right) \quad (6)$$

$N(0, 1)$, 设嵌入信息 $b_i (i=0, 1, \dots, L-1)$ 的取值是随机分布的, 那么扩频 CDMA 序列 W 的统计分布应服从正态分布 $W \sim N(0, L)$. 对 128bit 嵌入而形成的扩频序列进行统计分析, 在图 1 中左图是实验数据的分布情况, 并使用数据拟合软件进行分析, 图中曲线部分为拟合曲线, 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.

对上述多样本二元假设应用最大似然比估计检验, 则有

$$\ln \frac{p_Y(Y | H_1)}{p_Y(Y | H_{-1})} = \sum_{i=0}^{N-1} \frac{(y_i + g_i w_{j,i})^2 - (y_i - g_i w_{j,i})^2}{2\sigma^2} = \frac{2}{\sigma^2} \sum_{i=0}^{N-1} y_i g_i w_{j,i} \stackrel{H_1}{\geq} \tau \quad (7)$$

与直接使用伪随机序列 w_j 不同, 由此构造的检测器需要使用的水印权重因子为 g_i , 我们称其为带有匹配滤波的相关检测器 (matched filter correlator).

由于通信中受到干扰或攻击 n_i , 设接收端得到拷贝 S'' 经变换后表示为 $z_i = y_i + n_i$, 根据式 (7), 不考虑常数的影响, 使用匹配滤波的相关检测器计算的相关系数:

$$r_j = \frac{1}{N} \sum_{i=0}^{N-1} z_i g_i w_{j,i}, \quad j=0, 1, \dots, L-1 \quad (8)$$

嵌入水印信息可由如下判断公式得到

$$b_j = \begin{cases} 1, & r_j > \tau \\ \text{无水印}, & -\tau \leq r_j \leq \tau \\ -1, & r_j < -\tau \end{cases} \quad (9)$$

其中, τ 是检测阈值. 依据扩频 CDMA 水印检测模型, 下面分别对模型性能的几个方面给予讨论.

2.3 嵌入量对水印检测的影响

与原始图像信号 S 相比较, 在扩频 CDMA 水印模型中接收到的检测图像 S'' 不仅含有水印信息, 而且要受到量化噪声和信道噪声的干扰, 因而式 (8) 相关系数 r_j 可表示为

$$r_j = \frac{1}{N} \sum_{i=0}^{N-1} z_i g_i w_{j,i} = \frac{1}{N} \sum_{i=0}^{N-1} (x_i + n_i + \sum_{l=0}^{L-1} b_l g_i w_{l,i}) g_i w_{j,i} \quad (10)$$

设载体信号 x 、噪声 n 、每个扩频序列 w_i 彼此之间是相互独立的零均值高斯分布序列, 方差分别为 σ_x^2 、 σ_n^2 和 σ_w^2 , 则可以计算出 r_j 的期望为

$$\begin{aligned} E(r_j) &= \frac{1}{N} \sum_{i=0}^{N-1} E(z_i g_i w_{j,i}) \\ &= \frac{1}{N} \sum_{i=0}^{N-1} E\left[\left(x_i + n_i + \sum_{l=0}^{L-1} b_l g_i w_{l,i}\right) g_i w_{j,i}\right] \\ &= \frac{1}{N} \sum_{i=0}^{N-1} \left[E(g_i x_i w_{j,i}) + E(g_i n_i w_{j,i}) + \right. \\ &\quad \left. E\left(\sum_{l=0}^{L-1} b_l g_i^2 w_{l,i} w_{j,i}\right) \right] \\ &= \frac{1}{N} \sum_{i=0}^{N-1} b_j g_i^2 \sigma_w^2 = \frac{b_j \sigma_w^2}{N} \sum_{i=0}^{N-1} g_i^2 \end{aligned} \quad (11)$$

方差为

$$\begin{aligned} \text{var}(r_j) &= \frac{1}{N^2} \sum_{i=0}^{N-1} \text{var}(z_i g_i w_{j,i}) \\ &= \frac{1}{N^2} \sum_{i=0}^{N-1} \left[E(z_i g_i w_{j,i})^2 - E^2(z_i g_i w_{j,i}) \right] \\ &= \frac{1}{N^2} \sum_{i=0}^{N-1} \left\{ E\left[\left(x_i + n_i + \sum_{l=0}^{L-1} b_l g_i w_{l,i}\right) g_i w_{j,i}\right]^2 - b_j^2 g_i^4 \sigma_w^4 \right\} \\ &= \frac{1}{N^2} \sum_{i=0}^{N-1} \left[E(x_i^2 g_i^2 w_{j,i}^2) + E(n_i^2 g_i^2 w_{j,i}^2) + \right. \\ &\quad \left. E\left(\sum_{l=0}^{L-1} b_l^2 g_i^4 w_{l,i}^2 w_{j,i}^2\right) - g_i^4 \sigma_w^4 \right] \\ &= \frac{1}{N^2} \sum_{i=0}^{N-1} g_i^2 \left[\sigma_x^2 \sigma_w^2 + \sigma_n^2 \sigma_w^2 + \left(\sum_{l=0, l \neq j}^{L-1} g_i^2 \sigma_w^4 + g_i^2 E w_{j,i}^4\right) - g_i^2 \sigma_w^4 \right] \\ &= \frac{1}{N^2} \sum_{i=0}^{N-1} g_i^2 \left[\sigma_x^2 \sigma_w^2 + \sigma_n^2 \sigma_w^2 + (L-1) g_i^2 \sigma_w^4 + g_i^2 \sigma_w^2 \right] \end{aligned} \quad (12)$$

其中, σ_w^2 为扩频水印序列平方的方差. 对于本文的

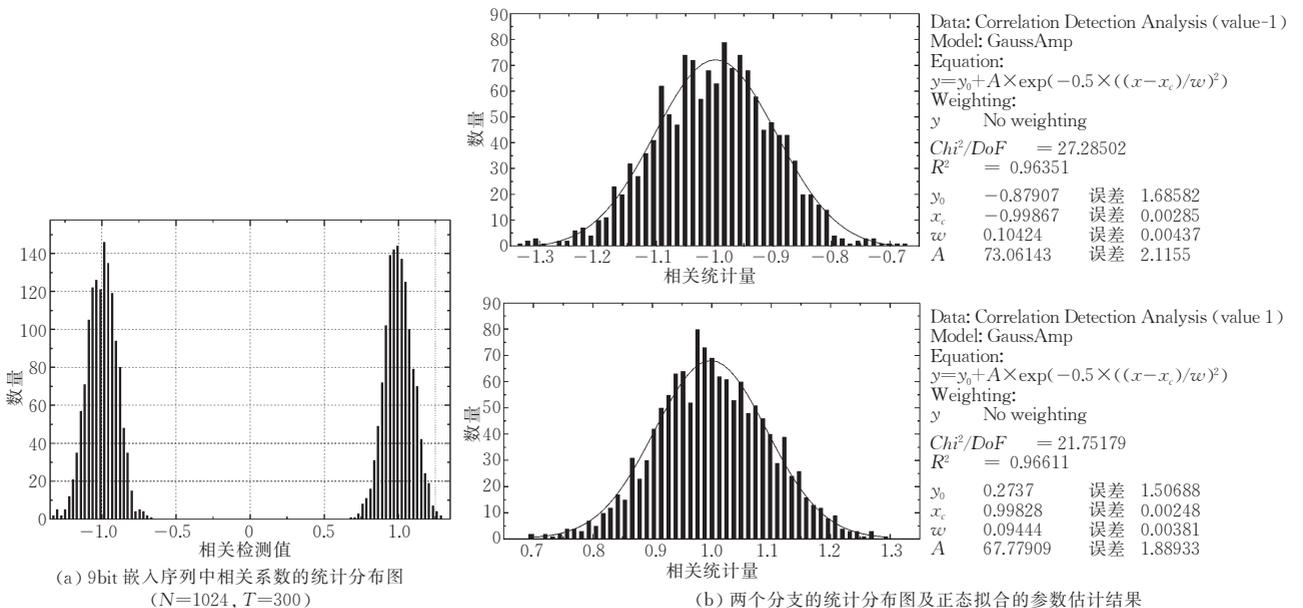
CDMA 扩频序列满足 $w \sim N(0, \sigma_w^2)$, 根据高斯分布的统计性质, 那么序列平方的方差为 $\sigma_w^2 = 2\sigma_w^4$, 因而相关系数 r_j 的方差可表示为

$$\begin{aligned} \text{var}(r_j) &= \frac{1}{N^2} \sum_{i=0}^{N-1} g_i^2 \left[\sigma_x^2 \sigma_w^2 + \sigma_n^2 \sigma_w^2 + (L+1) g_i^2 \sigma_w^4 \right] \\ &= \frac{\sigma_w^2}{N^2} \sum_{i=0}^{N-1} g_i^2 \left[\sigma_x^2 + \sigma_n^2 + (L+1) g_i^2 \sigma_w^2 \right] \end{aligned} \quad (13)$$

当 $L=1$, 退化为一般扩频水印. 不能看出, 嵌入量 L 的增加, 不影响相关系数的期望, 但是会使方差增大, 最终将增加检验的错误概率. 当水印序列、噪声、原图像为高斯分布时, 根据中心极限定理, 那么 r_j 近似可认为是均值为 $E(r_j)$ 、方差为 $\text{var}(r_j)$ 的高斯分布随机变量. 不失一般性, 当水印权重因子 $g_i = 1$ ($i=0, 1, \dots, N-1$) 时, 相关系数的分布满足

$$r_j \sim N\left(\pm \sigma_w^2, \frac{\sigma_x^2 + \sigma_n^2 + (L+1) \sigma_w^2 \sigma_w^2}{N}\right) \quad (14)$$

由此可见, 扩频序列的长度 N 和信息嵌入量 L 决定了检测性能, 载体信号和噪声信号同等地起到了干扰检测的作用, 序列长度对性能影响较大, 在参数确定的情况下, 增加水印序列长度显然能减少方差, 但是必须注意, 序列长度对方差的影响是平方根关系, N 越大, 影响越缓慢. 对正态分布 $N(\mu, \sigma^2)$ 来说, 事件将以较高的概率落入区间 $[\mu - 3\sigma, \mu + 3\sigma]$ 之中, 因此, 为保证错误概率足够小, 应当保证 $N \geq 9(\sigma_x^2 + \sigma_n^2 + (L+1)\sigma_w^2)$. 实验发现, 多小波分解图像高频子带的方差 $\sigma_x \in [5, 10]$, 再考虑到可能遇到的噪声影响, 建议 $N \geq 512$. 同时, 嵌入量 L 并不与序列长度 N 成正比, 当图像失真大小固定时, 增大 L 并不需



要 N 成倍增加, N 的增加并不大, 可据此提高水印容量。

为了通过实验来验证公式的正确性, 在没有任何干扰情况下, 即 $\sigma_x^2 = \sigma_n^2 = 0$, 将 $L = 9$ bit 的信息嵌入长 $N = 1024$ 的扩频序列中, 再使用模型中的方法进行检测, 为得到统计结果, 进行 300 次实验, 其相关检测的结果如图 2(a) 所示, 可以看到相关检测具有很好的区分性。在图 2(b) 将靠近 $\{-1, 1\}$ 两部分分别进行正态拟合, 其结果见图中右侧, 方差近似等于 0.0993, 这与 $\sigma = \sqrt{(L+1)/N} = 0.0988$ 是一致的。

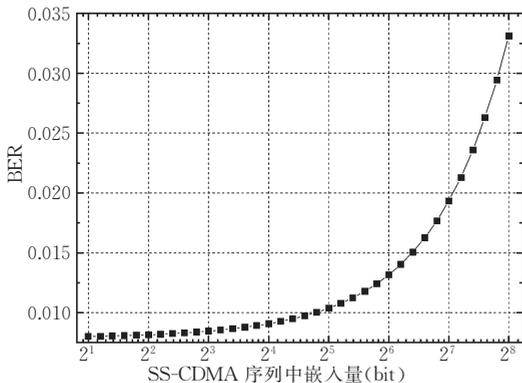
2.4 误码率和水印容量分析

虽然时域图像本身分布并不服从某种特定分布, 但是图像在变换域内却能表现出很好的分布特征, 因此假设信道噪声和载体作品在变换域下服从均值为 0 的高斯分布, 那么, 每一比特 b_i 对应的相关系数 r_i 也满足高斯分布, 令 $\mu = \sigma_w^2$, $\sigma^2 = (\sigma_x^2 + \sigma_n^2 + (L+1)\sigma_w^2)\sigma_w^2/N$, 则由式(14)有 $r_i \sim N(\pm\mu, \sigma^2)$ 。更为一般地, 将水印检测问题看作在两元假设 H_{-1} 和 H_1 中的参数检验问题, 其中 H_{-1} 表示存在比特信息 $b_i = -1$, H_1 表示存在信息 $b_i = 1$, 这样二元假设可以表示为

$$\begin{cases} H_1: r_i \sim N(\mu, \sigma^2) \\ H_{-1}: r_i \sim N(-\mu, \sigma^2) \end{cases}, i=0, 1, \dots, L-1 \quad (15)$$

那么, 对于某一给定的阈值 τ , 比特错误率(BER)可计算如下:

$$\begin{aligned} P_{\text{error}} &= P(r_i < -\tau | b=1)P(b=1) + P(r_i > \tau | b=-1)P(b=-1) \\ &= \frac{1}{2} \frac{1}{\sqrt{2\pi}\sigma} \int_{-\infty}^{-\tau} \exp\left(-\frac{(r_i - \mu)^2}{2\sigma^2}\right) dr + \frac{1}{2} \frac{1}{\sqrt{2\pi}\sigma} \int_{\tau}^{\infty} \exp\left(-\frac{(r_i + \mu)^2}{2\sigma^2}\right) dr \\ &= 2 \left(\frac{1}{2} \frac{1}{\sqrt{2\pi}\sigma} \int_{\tau}^{\infty} \exp\left(-\frac{(r_i + \mu)^2}{2\sigma^2}\right) dr \right) \end{aligned}$$



(a) 水印嵌入量对比特错误率(BER)的影响 ($N=2048, \sigma_w^2=300$)

$$= Q\left(\frac{\tau + \mu}{\sigma}\right) \quad (16)$$

其中, $Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^{\infty} \exp\left(-\frac{t^2}{2}\right) dt$ 。在 $b_i = 1$ 和 $b_i = -1$ 检测概率相等的情况下, 不妨假设 $\tau = 0$, 那么 BER 可以定义如下:

$$P_{\text{error}} = Q\left(\frac{E(r_i)}{\sqrt{\text{var}(r_i)}}\right) \quad (17)$$

根据式(11)和式(12), 当水印权重因子为常数 1 时, 可得扩频 CDMA 水印模型的错误概率为

$$P_{\text{error}} = Q\left(\sqrt{\frac{N}{\sigma_x^2 + \sigma_n^2 + (L+1)\sigma_w^2}} \sigma_w\right) \quad (18)$$

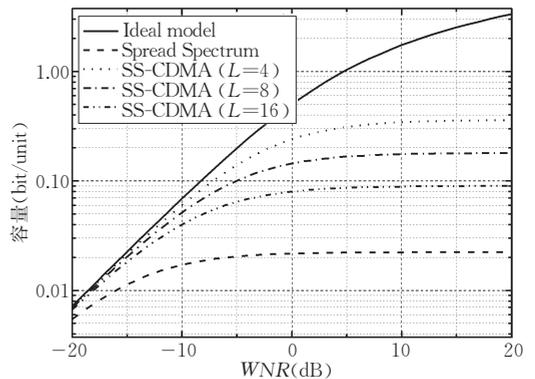
由此可见, 检测错误概率与扩频长度 N 成反比, 与信息嵌入量 L 成正比。在扩频长度 $N = 2048, \sigma_x^2 = 300, \sigma_w^2 = 1$ 时, 信息嵌入量 L 与比特错误率的关系见图 3(a) 所示, 随着 L 增加错误概率增大。

就水印容量而言, 根据 Costa 的脏纸理论, 假设通信信道受到两个独立的高斯噪声源的干扰, 一个干扰源 S 对发送者是已知的, 被称为参考源, 另一个干扰源 N 对各方是未知的, 被称为噪声源。发送方的输入 X 是与 S 相关的并且满足某种功率限制 $X \leq P_x$, 最终, 接收方的输入是 $Y = X + S + N$, Costa 指出这种信道的通信容量为 $\frac{1}{2} \log_2(1 + P_x/P_n)$, 并与参考源 S 无关, 其中 P_c 是干扰源功率。同样, 可以得到扩频水印理论上的容量为

$$C_{ss} = \frac{1}{2} \log_2\left(1 + \frac{\sigma_w^2}{\sigma_e^2 + \sigma_x^2}\right) \quad (19)$$

在相同嵌入条件下, 当扩频 CDMA 水印嵌入量为 L 时, 水印容量扩大 L 倍, 但扩频序列分布发生了改变, 正如式(4)所示, 每条子序列的方差缩小为 $\sigma_w^2 = \sigma_w^2/L$, 从而, 扩频 CDMA 水印的容量可表示为

$$C_{\text{cdma}} = \frac{L}{2} \log_2\left(1 + \frac{\sigma_w^2/L}{\sigma_e^2 + \sigma_x^2}\right) \quad (20)$$



(b) 不同水印模型容量的比较 ($DWR=15$ dB)

图 3 水印算法性能分析

在文档水印比 $DWR = \sigma_x^2 / \sigma_w^2$ 已知的情况下, 水印噪声比 $WNR = \sigma_w^2 / \sigma_e^2$ 与水印容量的关系如图 3(b) 所示, 图中有理想水印模型、扩频水印以及嵌入量 L 为 4, 8, 16 下的扩频 CDMA 水印容量, 与扩频水印比较, 随着 L 减小, CDMA 水印容量更加接近于理想水印模型容量, 特别在水印噪声比较低的时候, 但是每条扩频序列方差将减少 L 倍, 根据前面分析, 水印鲁棒性降低, 检测错误率增加。

3 基于多小波的数字水印

本节我们提出一种在多小波变换域下的新颖数字水印算法。从第 2 节扩频 CDMA 水印模型的理论分析中, 提高水印算法的性能, 除了要有好的水印嵌入/检测技术, 下面两个因素也决定了算法性能:

(1) 载体信号应当满足优良的分布特征, 如在扩频 CDMA 水印模型的分析中, 我们假定载体信号 x 满足均值为 0 的高斯分布, 即 $x \sim N(0, \sigma_x^2)$, 这种假定不仅具有普遍性, 而且有利于提高检测精度、降低错误率、减少因载体不同而对算法产生的影响、方便理论分析和实验研究;

(2) 必须能够最大限度地利用载体信号(参考源)信息来增强水印嵌入的性能(不可感知性、鲁棒性、容量), 如水印模型中水印权重因子 g_i (见式(2))是从参考源求得的先验知识, 不仅关系到图像的感知效果, 而且由式(11)和式(12)不难看出增大 g_i 将增大相关系数的均值, 从而提高水印检测精度。

为了达到这两个要求, 首先, 需要选择适当的嵌入域, 使它满足较好的统计特征; 同时, 需要实现某种感知模型, 来最大化地应用参考源的信息。下面将给出基于多小波的数字水印总体结构, 在此基础上阐述所提出的视觉掩蔽模型、水印嵌入算法和提取算法。

3.1 基于多小波的 CDMA 水印框架

图像处理通常希望得到紧支、对称、正交的变换形式, 标量小波变换很难同时满足这些性质, 为了达到这个目的, 提出了将单尺度函数生成的多分辨率空间推广到多尺度函数生成的多分辨率空间的多小波变换。多小波变换与小波变换相比更具一般性, 首先, 滤波器系数是矩阵而不是标量; 其次, 可以方便地构造尺度因子 m 大于 2 的多小波。这些差异使得多小波的构造比传统标量小波构造提供了更大的自由度以及更优越的性质, 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地利用这些额外的自由度。由 Donovan, Geronimo, Hardin 和 Massopust 构造了 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、对称性、尺度函数的整数平移相互正交等显著的特点, 本文也将在 DGHM 多小波基础上进行研究。

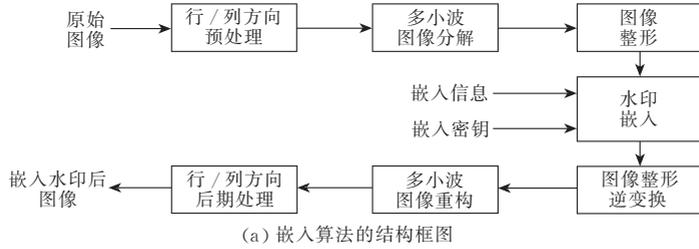
针对扩频 CDMA 数字水印, 我们期望图像经过多小波变换后在两个方面满足水印算法需要, 首先, 图像经多小波变换后, 由高频到低频分解为多层、多个子带, 每个高频子带 (HL, LH, HH) 表征了图像的细节信息, 并且统计分布近似服从高斯分布, 可以作为水印嵌入域; 其次, 变换后的低频层逼近系数表征了图像的基本信息, 将其与视觉感知模型结合, 能够获得较为精确的水印嵌入强度, 将它称为参考域。图像在多小波变换下的高频子带具有很好的分布特征, 如图 4(b) 所示, 分别是“Lena”图像 2 层分解 6 个高频子带的分布图, 可以看出分布近似服从均值为零的高斯分布, 符合扩频 CDMA 水印对嵌入域的要求, 同时, 与一般小波变换相比较, 其分布更近似于高斯分布。

多小波变换虽然具有优良的信号分析能力, 但是与小波变换比较, 它需要更加精细的处理过程, 因而增加了实现的复杂性。这些处理过程包括: 预处理 (preprocess)、边界处理 (handle boundaries)、图像整形 (resharpe)、后期处理 (postprocessing) 等。多小波预处理是指从一个给定的标量数据流生成 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、消失矩、频率响应和对称性是几个需考虑的因素, 考虑到正交性和消失矩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, 本文采用 Hardin-Roach 预滤波器来保留 2 阶消失矩和正交性。对图像变换而言, 数据是有限序列, 同时考虑到水印应用的要求, 需要在多小波变换后对数据进行整理, 整理包括边界处理、图像整形等。边界处理的方法有对称扩展法、矩阵完成法、边界函数法, 本文中采用对称扩展法, 它具有保留信号的连续性的特点; 图像整形是一种对每一子带在行方向和列方向分别进行下采样的方法, 将混杂的数据分解到各子带中的算法。

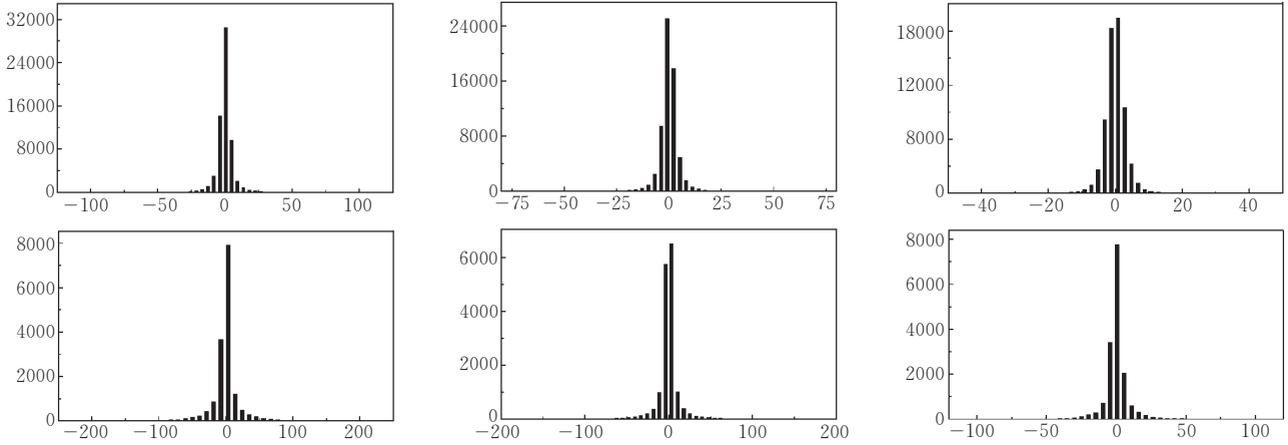
根据前面对图像多小波变换和扩频 CDMA 技术的分析和研究, 我们提出了一种基于视觉感知模型的扩频 CDMA 数字水印方案, 算法流程如下: 首先, 原始图像 S 经行/列两方向的 Hardin-Roach 预处理后, 进行 K 层 DGHM 多小波分解, 经图像整形处理得到载体图像 C_s , 再将 C_s 按照分解层 $l \in \{1, 2, \dots, K\}$ 、方向 $\theta = \{HL, LH, HH\}$ 和嵌入长度 N 分成几个嵌入块 $C_s^{l, \theta, r}$ ($r \in \mathbb{N}$), 然后使用扩频 CDMA 水印算法将负载信息 M 按照水印密钥 Key 嵌入到各嵌

入块中(每块中嵌入 L 比特信息),最后经过图像整形的逆变换、多小波反变换和行/列方向的后期处理得到最终的含水印图像 S' ,图 4(a)中给出了嵌入算法的结构框图. 与水印的嵌入算法类似,水印信息检测和提取采用盲水印方案,水印信息的提取过程如

下:对待检测的图像 S'' 经行列方向的预处理后,进行 K 层多小波分解,在图像整形处理后得到图像 C_s 并划分成嵌入块 $C_s^{l,\theta,r}$. 同时,按照水印密钥 Key 构造每块对应的 L 个伪随机序列,最后根据扩频 CDMA 水印的检测算法提取信息.



(a) 嵌入算法的结构框图



(b) LENA 图像的 3 层多小波分解后 6 子带分布图

图 4 多小波水印嵌入框图

3.2 视觉掩蔽模型

数字水印算法要更好地完成不可感知和鲁棒性两种性质,就要求水印权重因子自适于图像内容,因而理解人类的视觉系统从而构造水印嵌入的视觉模型是必须的. 影响视觉的因素主要有亮度掩蔽、对比度掩蔽和敏感度^[11],这里根据视觉的对比度和掩蔽效应,提出一种基于多小波变换的视觉掩蔽模型.

由于小波系数的多样性,在 DMWT 域下还没有统一的视觉模型,所提出的模型都是与具体的小波变换相关的. 在特定的分解层 l 和方向 $\theta = \{HL, LH, HH\}$ 中的坐标 (x, y) 处的小波分解系数的水印增益可表示为

其中, $x_{dc}(\tilde{x}, \tilde{y})$ 是坐标 (x, y) 在最低层 DMWT 低通子带对应像素点 (\tilde{x}, \tilde{y}) 的幅值模, $k_{l,\theta}$ 和 $C_{l,\theta}$ 为子带相关常数,具体数值见表 1,表中 k_0 取值依靠实际图像进行选择,范围在 0.5~1,一般情况下缺省值为 0.9.

表 1 多小波变换下视觉掩蔽模型常数表

层数	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

4 实验与分析

本实验以 512×512 的“Lena”图像为测试图(彩色图像可分别使用 RGB 子图),在 Matlab 下完成程序实现,多小波选用常见的 DGHM 小波,进行两层分解,感知掩蔽模型如前所述. 实验采用本文所提出的 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,这里将第 2 层的嵌入信息量减少 4 倍. 实验过程分解图例如图 5 所示,(a)为原始“Lena”图像,(b)为

$$g^{l,\theta}(x, y) = \beta(x, y) \sqrt{k_{l,\theta}^2 |x(x, y)|^2 + C_{l,\theta}^2} \quad (21)$$

其中, $\overline{x(x, y)}$ 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

$$\beta(x, y) = 3.62 (|x_{dc}(\tilde{x}, \tilde{y})| - 0.59)^2 + 0.68 \quad (22)$$

预处理后图像,(c)为 2 层多小波分解后图像,(d)为添加水印后,多小波反变换图像,(e)为后期处理后得到的最终嵌入水印图像,(f)是嵌入水印前后图像的差异.

差异.可以看出,人眼无法感知嵌入水印前后图像(a)和图像(e)之间的差异,此外,图 5(f)说明本文所使用的感知模型是有效的,能够较好地产生增益系数.

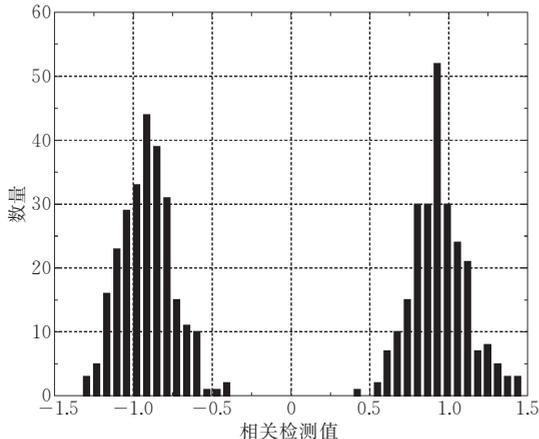


图 5 水印嵌入的处理过程

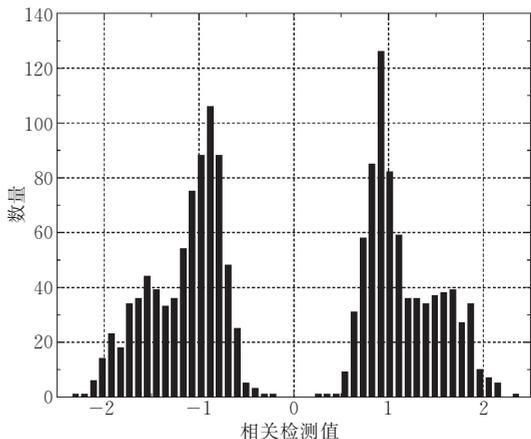
水印的检测性能是数字水印的核心问题,式(14)给出了我们所提出匹配滤波相关检测系数的分布情况,在实际应用中必须考虑到载体信号和信道噪声的影响,多小波变换的高频分解子带中,载体信号和信道噪声的分布都近似服从均值为零的高斯分布,因而方便进行定量分析和控制.为了说明算法的性能,我们对图像进行 2 层多小波分解,令扩频序列长 $N=2048$,每块中嵌入 $L=16\text{bit}$ 信息,所有嵌入信息之和为 $M=1632\text{bit}$.相关系数的分布情况如图 6 所示,其中图 6(a)为第 1 层 HL 子带的分布直方图,图 6(b)为两层所有嵌入信息的分布直方图,图中零值左右两侧各出现相连的两个近似正态分布,这是由于图像第 1 层与第 2 层分解系数的分布不同所致,第 2 层的感知权重要略大于第 1 层的权重

(见式(11)),因此分布图中偏离零点更远.总之,由图 6 可知,式(14)正确反映了相关检测的分布情况.

水印嵌入量 L 和扩频序列长度 N 是改善水印系统性能的重要因素,为了测试嵌入量对水印的影响,我们保持扩频序列长度 $N=2048$ 不变,由小到大改变嵌入量 L 大小,观察比特错误概率(BER)的变化,实验结果如图 7(a)所示,图中曲线表明,随着嵌入量的增加,错误概率增大,与图 3(a)理论分析的结果相比较,基本是一致的,实验中错误率上升比理论值快,说明嵌入量的增大改变了图像的某些分布特征(如量化噪声等),从而增加了错误率.为了测试扩频序列长度对水印性能的影响,我们保持 $L=16\text{bit}$ 不变,改变每块中嵌入长度 N 的大小,并对嵌



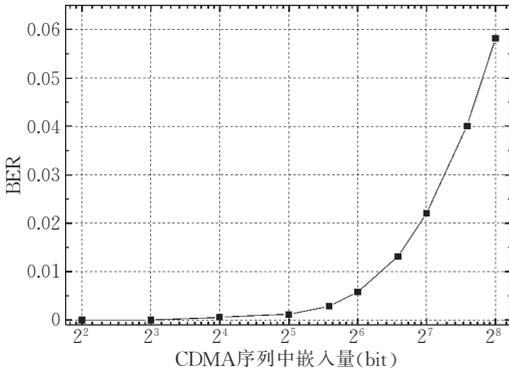
(a) 第 1 层 HL 子带相关系数的统计分布图



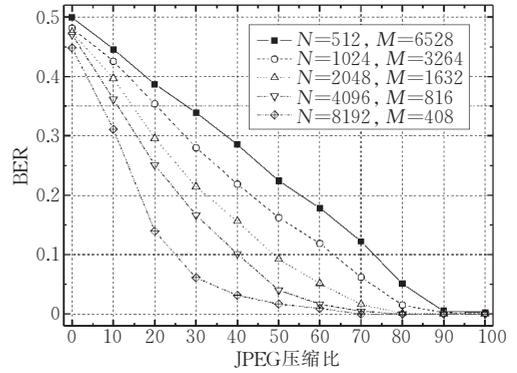
(b) 2 层 DMWT 分解, $N=2048$ 及 $L=16$ 的相关系数统计分布图

入水印的图像进行 JPEG 压缩, 观察比特错误概率 (BER), 实验结果如图 7(b) 所示, 其中 M 为整个图像的信息嵌入量 (bit), 图中数据表明, 随着长度的增加, 鲁棒性增强, 错误率下降, 但是嵌入量减少. 总

之, 嵌入量 L 和扩频序列长度 N 两者间存在互补的制约关系, 增大嵌入量 L 在增加通信容量的同时也增加了载体失真, 然而, 随着长度 N 的增加, 水印的错误率下降、鲁棒性显著增强, 但容量降低.



(a) 嵌入量 L 对比特错误概率 (BER) 的影响 ($N=2048$)



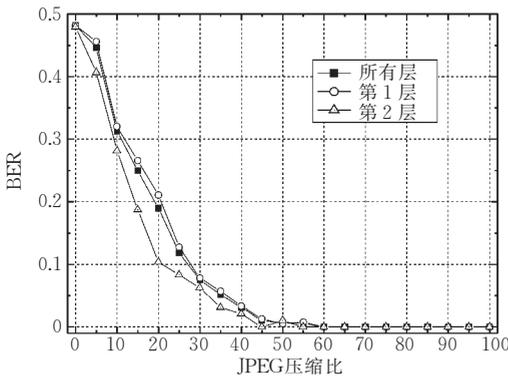
(b) 嵌入量、扩频序列长度 N 对比特错误概率 (BER) 的影响 ($L=16\text{bit}$)

图 7

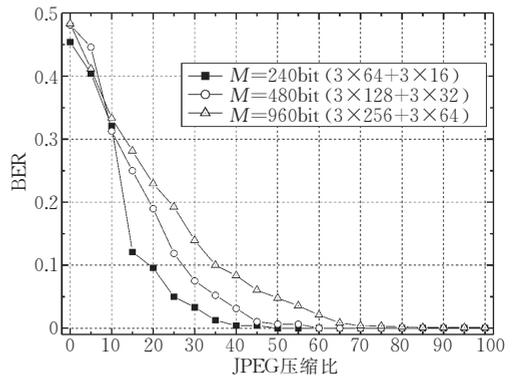
为了检验算法的鲁棒性, 采用 JPEG 有损压缩来检验算法, 这里 JPEG 压缩算法是 Matlab 中的压缩算法, 压缩强度在 10%~100% 之间. 在保证不可感知的前提下, 我们采用中等强度进行嵌入, 对 480bit 信息嵌入 (第 1 层为 $3 \times 128\text{bit}$, 第 2 层为 $3 \times 32\text{bit}$) 的实验结果见图 8(a) 所示, 可以看出本算法具有很强的抵抗 JPEG 压缩能力, 在压缩率达到 35% 仍然有很好的性能. 同时, 图中给出了第 1 层和第 2 层的鲁棒性对比结果, 可以看出, 第 2 层结果要好于第 1 层, 这是因为第 2 层频率更低, 含有更多

感知重要的成分, 被压缩保留下来的信息更多的结果.

与一般的扩频水印相比较, 本文提出的算法既具有很强的鲁棒性, 又有更大的容量, 为了检验算法的容量和鲁棒性之间的关系, 我们分别嵌入 240bit, 480bit, 960bit 的负载, 并在 JPEG 压缩下观察其比特错误率的变化情况, 其结果见图 8(b) 所示. 不难看出, 随着负载的降低, 鲁棒性能增强, 特别是小负载下, 基本不受 JPEG 压缩的影响, 即使在 JPEG 压缩 50% 的情况下也无妨.



(a) 480bit 及 2 层水印嵌入



(b) 240bit, 480bit, 960bit 及 2 层水印嵌入 (扩频长度 $N_1=65536$, $N_2=16384$)

图 8 JPEG 压缩下的 BER 变化

扩频技术具有良好的抗缩放、裁减和滤波等性质^[1], 扩频 CDMA 水印是在此基础上提出的, 实验中发现它也能够有效地抵抗这些处理或攻击, 例如在图 9 中, 将 (a1) 中 32×32 的 2 值图像作为水印嵌入图像, (b1) 和 (b2) 分别为剪切后图像和被恢复的信息图像, (c1) 和 (c2) 分别为修改后图像和被恢复的信息图像, 可见扩频 CDMA 水印具有较强抵抗攻击的能力. 总之, 本文提出的算法具有较强鲁棒性又有较大嵌入容量, 同时图像没有明显的失真.



图 9 在剪裁和修改攻击后的含水印图像及其嵌入信息变化

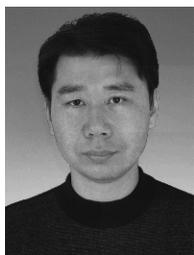
5 结 论

本文较系统地分析了扩频 CDMA 水印模型的性能以及各种指标之间的制约关系,并在多小波变换和图像多小波视觉掩蔽模型基础上,在保证鲁棒性前提下,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扩频 CDMA 数字水印方案.大量实验结果表明所提出的算法既具有较高嵌入容量,又具有较强的鲁棒性,从而验证了理论分析的正确性.本文的结论对于相关领域中的数字水印实现也具有指导意义.

参 考 文 献

- 1 Cox I. J. , Kilian J. , Shamoon T. , Leighton T. . Secure spread spectrum watermarking for multimedia. *IEEE Transactions on Image Processing*, 1997, 6(12): 1673~1687
- 2 Vassaux B. , Bas P. , Chassery J.-M. . A new CDMA technique for digital image watermarking enhancing capacity of insertion and robustness. In: *Proceedings of IEEE International Conference on Image Processing*, Greece, 2001, 3: 983~986
- 3 Silvestre G. C. M. , Dowling W. J. . Embedding data in digital images using CDMA techniques. In: *Proceedings of the 7th IEEE International Conference on Image Processing*, Vancouver, Canada, 2000, 1: 589~592
- 4 Moulin P. , O'Sullivan J. A. . Information-theoretic analysis of

- information hiding. *IEEE Transactions on Information Theory*, 2003, 49(3): 563~593
- 5 Hernández J. R. , Pérez-González F. , Rodríguez J. M. , Nieto G. . Performance analysis of a 2D-multipulse amplitude modulation scheme for data hiding and watermarking of still images. *IEEE Journal Selected Areas Communication*, 1998, 16(4): 510~524
- 6 Hernández J. R. , Amado M. , Pérez-González F. . DCT-Domain watermarking techniques for still images: Detector performance analysis and a new structure. *IEEE Transactions on Image Processing*, 2000, 9(1): 55~68
- 7 Chen B. , Wornell G. W. . Quantization index modulation: A class of provably good methods for digital watermarking and information embedding. *IEEE Transactions on Information Theory*, 2001, 47(4): 1423~1443
- 8 Chen B. , Wornell G. W. . Quantization index modulation methods for digital watermarking and information embedding of multimedia. *Journal of VLSI Signal Processing Systems*, 2001, 27(1~2): 7~33
- 9 Tham J. Y. , Shen L.-X. , Lee S. L. , Tan H. H. . A general approach for analysis and application of discrete multiwavelet transforms. *IEEE Transactions on Signal Processing*, 2000, 48: 457~464
- 10 Attakitmongkol K. , Hardin D. P. , Wilkes D. M. . Multiwavelet prefilters II: Optimal orthogonal prefilters. *IEEE Transactions on Image Processing*, 2001, 10(10): 1476~1487
- 11 Mayache A. , Eude T. , Cherifi H. . A comparison of image quality models and metrics based on human visual sensitivity. In: *Proceedings of International Conference on Image Processing(ICIP'98)*, 1998, 3: 409~413



ZHU Yan, born in 1974, Ph. D. .

His research interests include computer security, cryptography, information hiding, media security and pattern recognition.

SUN Zhong-Wei, born in 1969, Ph. D. , associate professor. His research interests include multimedia information

processing and information security.

YANG Yong-Tian, born in 1939, professor and Ph. D. supervisor. His research interests include computer network and application, distribution system and fault-tolerant computer system.

FENG Deng-Guo, born in 1965, professor and Ph. D. supervisor. His research interests include information security, network security and cryptography.

Background

The research of this paper is one part of the project "digital fingerprinting and application of Copyright Protection in Digital Multimedia". Digital fingerprinting is a new effective technology to resolve multimedia copyright protection in recent years. The project mainly focuses on efficient implementations of the fingerprinting scheme in three major do-

main: fingerprint embedding, coding and protocol designing. As an important part of fingerprint embedding, the research of this paper mainly helps to resolve the problem of channel capacity under the precondition of robustness and present a practical, feasible scheme for information hiding.