

# 多小波变换域内基于扩频和量化的混合水印研究

朱 岩<sup>1</sup>, 杨永田<sup>2</sup>, 冯登国<sup>3</sup>

(1. 北京大学计算机科学技术研究所, 北京 100871; 2. 哈尔滨工程大学计算机科学与技术学院, 黑龙江哈尔滨 150001; 3. 中科院研究生院信息安全国家重点实验室, 北京 100049)

**摘 要:** 考虑到扩频和量化技术存在互补性, 本文构造一种扩频和量化混合模型, 并提出了一种图像多小波变换域内基于扩频和量化的混合数字水印方案, 通过理论分析给出了扩频长度、信道容量、检测错误率等参数间的关系, 实验结果表明算法实现了水印鲁棒性前提下的水印容量最大化的目的。

**关键词:** 数字水印; 脏纸模型; 扩频; SCS; 多小波变换

**中图分类号:** TN391 **文献标识码:** A **文章编号:** 0372-2112 (2006) 10-1817-06

## Research on Hybrid Watermarking Based on Spread Spectrum and Quantization in Multiwavelet Domain

ZHU Yan<sup>1</sup>, YANG Yong-tian<sup>2</sup>, FENG Deng-guo<sup>3</sup>

(1. Institute of Computer Science and Technology, Peking University, Beijing 100871, China;

2. Computer Science and Technology School, Harbin Engineering University, Harbin, Heilongjiang 150001, China;

3. State Key Laboratory of Information Security, The Chinese Academy of Sciences, Beijing 100049, China)

**Abstract:** Considering both of Spread spectrum and quantization can complement, a hybrid watermarking model is constructed by integrating spread spectrum with quantization technique. Furthermore, a novel hybrid watermarking scheme is proposed based on spread spectrum and quantization in multiwavelet domain. The performance analysis is used to describe the interrelations among length of sequence, channel capability, detection error rate and so on. Moreover, the experimental results demonstrate that the proposed algorithm provides the capacity maximization under the precondition of robustness.

**Key words:** digital watermarking; dirty paper model; spread spectrum; scalar Costa scheme; multiwavelet transform

### 1 引言

扩频和量化是两种主要的水印技术, 通过使用水印理论模型, 如 Costa 脏纸模型<sup>[1,2]</sup>、Sullivan 和 Moulin 提出的竞争模型<sup>[3]</sup>等, 对扩频和量化技术的分析发现, 这两种技术在鲁棒性和水印容量方面存在互补关系。扩频水印具有鲁棒性强、高安全性、多水印嵌入的优点, 但是水印容量较低。Cox 等人<sup>[4]</sup>首先提出了扩频水印的思想, 并在各种攻击下对水印性能进行了分析和验证。为了改善性能, 一般将其应用到各种变换域中, 例如文献<sup>[5]</sup>将感知自适应水印嵌入图像小波变换域中。量化水印则是一种通过改变信号采样的量化值来隐藏。例如 Chen 等人提出了量化索引模型(QIM)<sup>[6,7]</sup>, 其基础是具有固定步长的均匀抖动量化器, 抖动在量化中引入了随机噪声保证了水印安全, 同时, 从理论上证明了模型的良好性能。在文献<sup>[8]</sup>中, Eggers 等人根据 Costa 理论模型提出了标量 Costa 方案, 方案用标量码书代替 Costa 模型中的随机码书, 并引入了缩放因子增加方案适用性。总之, 如何克服扩频和量化水印的缺点

并发挥各自的优点是当前研究的热点。

除了数字水印算法以外, 如何有效地实现数字算法也是一个极其重要的问题。在 Costa 脏纸模型中, 水印码书的编码要由嵌入信息分布和载体信号(参考源)对编码方式的影响来确定, 其中, 载体信号的统计特征是极其重要的因素, 一方面, 期望载体信号的统计特征能服从某种确定分布; 另一方面, 期望编码形式能充分利用载体信号的信息。本文基于这两方面的要求, 利用图像离散多小波变换(DMWT)的细节子带近似服从一般高斯分布的性质, 以及使用视觉掩蔽模型达到水印自适应嵌入的目的设计一种新颖的数字水印。

本文在水印鲁棒性前提下以最大化水印容量为目标构造出一种新颖的水印方案。在第 2 节中, 根据扩频水印和量化水印的优缺点存在互补性, 构造一种新颖的组合扩频和量化技术的混合水印模型; 第 3, 4 节提出了一种图像多小波变换域内的混合数字水印方案, 并依靠 Costa 脏纸模型对模型性能进行了理论分析; 第 5 节对水印性能进行了实验验证和参数选择与分析, 最后总结全文。

## 2 基于量化和扩频的水印模型

本节在 Costa 模型基础上对扩频和量化水印进行比较和分析,提出一种混合扩频和量化技术的水印算法,并给出详尽的水印嵌入和检测过程.

### 2.1 Costa 水印模型

Costa 脏纸模型如图 1 所示,假设通信信道受到两个独立高斯噪声源干扰,一个干扰源  $x$  对发送者是已知的,称为载体信号,另一个干扰源  $e$  对各方是未知的,称为干扰源.发送方的输入  $w$  与  $x$  相关并且满足某种功率限制  $w \leq P_w$ ,最终,接收方的输出为  $y = w + x + e$ .Costa 指出这种信道的通信容量为  $\frac{1}{2} \log_2 \left( 1 + \frac{P_w}{P_e} \right)$ ,且与参考源  $w$  无关,其中  $P_e$  是干扰源功率.载体信号  $x$  和干扰源  $e$  是独立高斯分布,分别具有方差  $\sigma_x^2$  和  $\sigma_e^2$ .由于通信隐蔽性要求,携带信息的信号  $w$  的能量受到限制,即  $E(w^2) \leq P_w$ .为了达到最佳嵌入,主要的问题是附加变量  $U$  的设计,即解码码书设计.通常使用伪随机序列作为水印信号来构造码书,由文献[2]可知模型的信道容量可表示为:

$$C = \max_{p(x|p(u,w|x),p(y|w,x))} \{ I(u; y) - I(u; x) \} \quad (1)$$

其中,  $I(a, b)$  是在变量  $a$  和  $b$  之间的互信息.

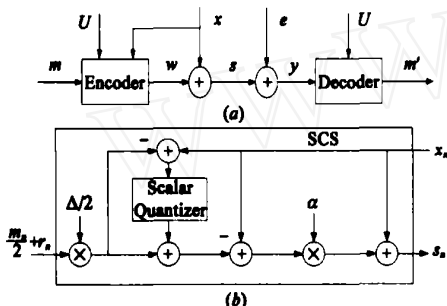


图 1 (a)水印通信模型和 (b)标量 Costa 方案的水印嵌入结构图

Costa 提出了一种理想随机码书模型:

$$U = \{ u = w + x \} \quad (2)$$

其中,  $w$  和  $x$  为独立随机过程,分别表示被嵌入信号和载体信号,每个分量满足  $w: N(0, \sigma_w^2)$  和  $x: N(0, \sigma_x^2)$ ,缩放因子  $\alpha$  满足  $\alpha \in (0, 1)$ ,理论上 最优值为  $\alpha = \sigma_w^2 / (\sigma_w^2 + \sigma_e^2)$ ,信道容量为

$$C_{ideal} = \frac{1}{2} \log_2 \left( 1 + \frac{\sigma_w^2}{\sigma_e^2} \right) \quad (3)$$

$C_{ideal}$  表示理想情况下的水印容量,取值为信道容量的上界.

扩频水印是将伪随机序列直接附加到载体信号中的一种水印技术,它的水印与码书是相同的,可以认为是  $u = w + \alpha x$  下的特殊情况,此时,  $U = \{ u = w \}$ ,信道容量为  $C_{ss} = \frac{1}{2} \log_2 \left( 1 + \frac{\sigma_w^2}{\sigma_e^2 + \sigma_x^2} \right)$ ,由于载体信号限制了容量,扩频水印容量是次优的.

另一种常见的水印技术是量化方法,对信号采样值的量化可认为降低了载体和噪声的方差,由式(3)可知具有更高的水印容量.通常的量化嵌入方法由于没有引入随机性,安全性

较差.因此,理想的量化水印需要在量化中引入随机噪声,目前实用的量化水印技术有量化索引模型(QIM)、标量 Costa 方案(SCS)等.在 SCS 方案中,使用标量码书代替式(2)中的随机码书,在二值情况下,标量码书为

$$U = \left\{ u = k + m \frac{r_n}{2} \mid m \in \{0, 1\}, k \in Z \right\} \quad (4)$$

其中,  $\Delta$  是量化步长,  $\alpha$  是缩放因子且  $\alpha \in (0, 1)$ ,  $k$  枚举所有量化步长为  $\Delta$  的量化值,  $m$  为量化平移.对 最优值的搜索过程简化为对码书  $U$  的量化过程,即  $q = w / \Delta = u / \Delta - x$ ,由此定义等式:

$$q_n = Q \left( x_n - \left( \frac{m_n}{2} + r_n \right) \right) + \left( x_n - \left( \frac{m_n}{2} + r_n \right) \right) \quad (5)$$

$Q(g)$  是具有量化步长  $\Delta$  的标量均匀量化器,  $r_n$  是伪随机数且  $r_n \in (0, 1)$ .最终,生成带有水印的数据  $s = x + w = x + \alpha q$ ,其嵌入过程的框图如图 1(b) 所示.

### 2.2 混合水印嵌入算法

以扩频与量化技术为基础,我们将自适应扩频水印和标量 Costa 方案(SCS)进行组合,提出一种混合水印算法,算法在载体信号与水印信号的归一化相关中进行 SCS 量化嵌入,再将量化结果扩频嵌入于载体信号中.由于 Costa 脏纸模型中码书编码由嵌入信息  $x$  的分布和参考源对编码方式的影响来确定,需要参考源的统计特征能服从确定分布,并且编码形式要充分利用参考源信息.因此本文将图像在变换域内分为两个区域:参考域和嵌入域.参考域使用视觉掩蔽模型达到水印自适应嵌入,嵌入域具有良好的统计分布特征用于隐藏信息.由于相关检测为在 Gaussian 分布下最优检测器,因此我们期望嵌

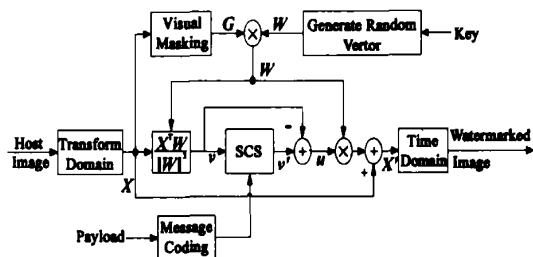


图 2 混合水印嵌入结构图

入域服从高斯分布.首先在变换域内将载体采样向量  $x$  与随机向量  $w$  归一化相关得到相关系数  $v$ ,再使用标量 Costa 方案(SCS)在  $v$  中嵌入一比特信息  $m$  得到  $u$ ,最后  $u$  对  $w$  进行缩放并用扩频方法嵌入到载体作品中,得到带水印的作品  $X$ ,结构框图如图 2 所示,其中 SCS 模块见图 1(b),视觉掩蔽模块用于计算感知自适应嵌入的水印增益  $G$ .具体的水印嵌入算法如下:

**E1** 将载体作品  $S$  分解到变换域,按照嵌入比特信息  $M = \{ m_1, m_1, \dots, m_N \} (m_i \in \{0, 1\})$  的数量将水印嵌入域分割成相等长度  $L$  的  $N$  块  $\{ X_1, X_2, \dots, X_N \}$ ,每块嵌入一位信息;同时,根据嵌入密钥  $K_{em}$ ,使用伪随机数发生器为每比特信息  $m_i$  生成一个随机向量  $W_i = \{ w_{i1}, w_{i2}, \dots, w_{iL} \}$ ,其长度与块  $X_i$  相同;

**E2** 使用视觉掩蔽模型依靠参考域求取图像块  $X_i$  对应的水印增益  $G_i = \{ g_{i1}, g_{i2}, \dots, g_{iL} \}$ ,根据增益调整随机向量  $W_i$ ,得到向量  $W_i = \{ g_{i1}w_{i1}, g_{i2}w_{i2}, \dots, g_{iL}w_{iL} \}$ ;然后,计算载体图像块  $X_i$  与随机向量  $W_i$

归一化相关的相关系数  $v_i$  为:

$$v_i = \frac{X_i^T \cdot W_i}{W_i^2}, i = 1, 2, \dots, N \quad (6)$$

其中,  $g$  为向量内积,  $|g|$  是向量的模.

E3 运用 SCS 算法,在相关系数  $v_i$  中对比特信息  $m_i$  进行量化嵌入,由式(5)得到:

$$v_i = v_i + \left[ Q \left( v_i - \left( \frac{m_i}{2} + r_i \right) \right) + \left( \frac{m_i}{2} + r_i \right) - v_i \right] \quad (7)$$

其中,  $Q(\cdot)$  是具有量化步长  $Q$  的标量均匀量化器,  $r_i$  是伪随机数且  $r_i \in (0, 1]$ ,  $Q$  是缩放因子.

E4 使用扩频技术,将随机向量  $W_i$  嵌入到载体图像块:

$$X_i = X_i + u_i W_i \quad (8)$$

其中,  $u_i = v_i - v_i$ . 将  $X$  与参考域部分结合,经图像反变换得到带水印图像  $S$ .

### 2.3 混合水印提取算法

当对某一载有水印的图像  $S$  提取它含有的信息时,需要执行水印提取算法.综合扩频和量化检测技术,在不需要原载体作品参与下,我们提出的盲水印提取算法如下:

D1 对接收到的图像  $S$  进行多小波变换,按照嵌入算法中的步骤 1 与 2,分别得到  $N$  个嵌入块  $X_i$ 、增益向量  $G_i$ 、随机向量  $W_i$ ,以及归一化相关系数  $v_i (i = 1, 2, \dots, N)$ . 这里水印的安全性是建立在生成随机向量  $W_i$  的水印密钥  $K_m$  之上,同时,信道干扰对增益向量  $G_i$  的改变可忽略不计.

D2 将每个相关系数  $v_i$  转化为软判决输出如下:

$$o_i = |Q(v_i - r_i) + r_i - v_i| \quad (9)$$

其中,  $o_i$  为软判决输出且  $o_i \in [0, 1/2]$ ,  $Q(\cdot)$  是具有量化步长  $Q$  的标量均匀量化器,  $r_i$  是由密钥产生的伪随机数.

D3 根据软判决  $o_i$ ,计算嵌入比特信息  $m_i$  的估计:

$$m_i = \text{sign} \left( o_i - \frac{A}{2} \right) \quad (10)$$

其中,  $\text{sign}$  为符号函数,正数为 1;否则为 -1. 如果  $m_i$  为 1,则嵌入信息为 1,否则  $m_i$  为 -1,信息为 0.

嵌入算法综合了扩频和量化两种技术,检测算法也包括扩频检测和量化检测两步,考虑到系统的稳定性,可以采用纠错码对嵌入信息进行编码,减少通信中出现的错误,同时,所提出的算法也可应用于时域图像中.

## 3 基于多小波的混合数字水印

在混合水印算法基础上,从嵌入域和感知自适应嵌入两方面对算法给予改进,本文提出一种多小波变换域下混合扩频和量化技术的新颖数字水印算法.

### 3.1 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  $\psi(x)$ ,而多小波变换<sup>[9]</sup>具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

$(x) = [ \phi_1(x) \ \phi_2(x) \ \dots \ \phi_r(x) ]^T (r = N)$  表示多分辨率分析空间  $\{V_k\}_k$  上的  $r$ -维多尺度函数,与其对应的多小波函数

$(x) = [ \psi_1(x) \ \psi_2(x) \ \dots \ \psi_r(x) ]^T$  构成了正交互补子空间上  $\{W_k\}$  的正交基,即  $W_j$  是  $V_{j+1}$  中的正交补空间.  $(x)$  和  $(x)$  满足下列二尺度差分方程

$$(x) = \sqrt{2} \sum_k H_k (2x - k), \quad (x) = \sqrt{2} \sum_k G_k (2x - k) \quad (11)$$

其中,  $\{H_k\}$  和  $\{G_k\}$  是  $r \times r$  矩阵滤波器. 则它们的双正交性条件可表示为

$$\begin{aligned} H_k H_k^* - ml &= G_k G_k^* - ml = 0I_r, & H_k G_k^* - ml \\ &= G_k H_k^* - ml = 0r \end{aligned} \quad (12)$$

其中“ $*$ ”为矩阵复共轭转置,  $I_r$  和  $0_r$  是  $r \times r$  单位阵和零矩阵.

多小波变换与小波变换相比更具一般性,其滤波器系数  $H_k$  是矩阵而不是标量,并且可以构造尺度因子大于 2 的多小波. 这些差异使得多小波构造比传统标量小波构造提供了更大的自由度,这些额外自由度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. 目前研究较多的是  $r = 2$  的多小波变换,由于 DGHM 多小波既保持了标量小波的良好时域和频域局部化特征,又具有紧支性、二阶逼近、多小波函数的对称和反对称性、多尺度函数对称性以及整数平移相互正交等显著的特点. 因此本文也将使用它进行分析.

### 3.2 基于多小波的混合数字水印

直观上看,图像多小波分解与标量小波分解的主要区别在于:在同一尺度、同一方向上存在对应不同小波的多个细节子带,通过对各子带的研究发现,细节子带的分布近似服从均值为零的高斯分布,并且视觉感知不明显,而低频子带分布不规则,保留了大部分视觉信息. 图像多小波变换的这些性质以及图像多小波视觉感知模型,满足了前面扩频和量化混合水印的两个要求. 嵌入域服从高斯分布和易于求得自适应嵌入的增益系数,在此基础上,我们提出了一种新颖的基于多小波变换的扩频和量化混合水印方案.

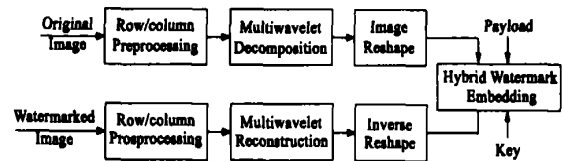


图 3 基于多小波的水印嵌入框图

完整的多小波混合水印算法流程如下:首先,原始图像经过行/列方向的预处理后进行多小波分解,再经图像整形处理得到载体图像,使用本文的混合水印算法将负载信息依靠密钥嵌入到载体图像中,然后,经过图像整形的逆变换、多小波反变换和行/列方向的后处理得到最终的水印图像,嵌入算法的结构图如图 3 所示. 水印检测算法流程与此类似,在预处理、多小波变换和图像整形之后,由混合水印提取算法恢复出隐藏信息.

## 4 性能理论分析

通过分析检测算法来说明混合模型的有效性,检测算法包括扩频检测和量化检测两步:首先,载有水印信号与随机信号的归一化相关检测,不考虑信道噪声影响,令  $X_i = X_i + u_i W_i$ ,归一化相关可表示为

$$v_i = \frac{X_i^T W_i}{W_i^2} = \frac{(X_i + u_i W_i)^T W_i}{W_i^2} = \frac{X_i^T W_i}{W_i^2} + u_i = v_i + u_i = v_i \quad (13)$$

其中,在嵌入算法中有  $u_i = v_i - v_i$ . 可知  $v_i$  是  $v_i$  经一比特信息

$m_i$  量化嵌入后结果. 其次, 依据式 (7) 中量化嵌入方法, 采用 SCS 水印检测公式进行量化检测, 见检测步骤 2 和 3, 将水印信息提取出来.

根据 Costa 脏纸理论, 缩放因子  $\alpha$  的最优选择对于实现通信容量和系统解码可靠性之间的平衡具有重要作用, 其最优值为  $\frac{2}{\sqrt{2}} / (\frac{2}{\sqrt{2}} + \frac{2}{e})$ . 经典 SCS 嵌入算法依靠两个参数: 量化步长  $\Delta$  和缩放因子  $\alpha$ . 在附加高斯白噪声信道 (AWGN), 对于给定的  $\Delta$  和嵌入失真  $\frac{2}{\sqrt{2}}$ , 令水印在量化间隔内均匀分布, 则量化步长可以表示为  $\Delta = \sqrt{12} \frac{2}{\sqrt{2}}$ . 可以推导出最优嵌入下,

$$C_{SCS} = \frac{1}{2} \log_2 \left[ 1 + \frac{2}{2.71 \frac{2}{e}} \right] \quad (14)$$

显然, 当水印噪声比  $WNR = \frac{2}{\sqrt{2}} / \frac{2}{e}$  大于零时, 这种近似性较好.

对于本文所提出的算法, 是一种将扩频技术与量化技术相结合的混合方法, 与 SCS 中的  $C_{SCS}$  相比较, 扩频水印算法中缩放因子  $\alpha_{SS} = 0$ , 因此通过混合两种算法, 能够使得更接近于理论上的最优值. 令扩频因子  $L$  表示  $x$  与  $w$  相关的序列长度, 提出算法中信息并不直接嵌入到载体信号  $x$  中, 而是嵌入到扩频序列  $w$  的相关系数中, 因此, 算法性能与  $L$  直接相关. 在理想模型下, 假定信道噪声  $e$  与扩频序列  $w$  正交, 对于攻击者, 在不知道扩频序列的情况下, 必须添加足够大的失真才能影响水印信息. 因此, 可以证明水印噪声比  $WNR$  与扩频因子  $L$  成反比, 同时, 信道容量与扩频因子  $L$  成反比. 因而, 在高斯信道 (AWGN) 上的信道容量可近似表示为

$$C = \frac{1}{2L} \log_2 \left[ 1 + \frac{L \cdot \frac{2}{\sqrt{2}}}{(1.71 + 1/L) \frac{2}{e}} \right] = \frac{1}{2L} \log_2 \left[ 1 + \frac{WNR \cdot L}{1.71 + 1/L} \right] \quad (15)$$

不难看出, 当  $L = 1$  时退化为量化嵌入. 根据通信信道的不同, 参数取值也不同, 当  $WNR$  较小时,  $L$  可以选择较大, 其特征类似于量化嵌入; 当  $WNR$  较大时,  $L$  的取值可以较小, 类似于扩频嵌入. 在图 4(a) 中给出了高斯信道下扩频因子  $L = 15$  的混合模型信道容量曲线, 以及模型的容量包络曲线 (信道容量上限曲线), 与扩频水印 (SS) 和 SCS 算法比较, 包络曲线综合了两者的优点, 在高  $WNR$  时接近量化曲线, 在低  $WNR$  时接近扩频曲线, 因而更接近于理想盲水印容量.

量化步长  $\Delta$  的选择直接影响到水印的效果, 在量化水印中影响缩放因子  $\alpha$ , 即增大  $\Delta$  则图像失真增加, 并且量化步长  $\Delta$  控制量化码书间距大小, 缩小  $\Delta$  将使检测性能下降. 假设在归一化相关后伪随机序列在每个量化步长上均匀分布, 根据均匀分布的统计性质, 水印的方差可以表示为  $\sigma_w^2 = \frac{2}{12}$ , 由于  $\Delta$  在量化中的缩放作用, 则有  $\sigma_w = \sqrt{12} \frac{\Delta}{\sqrt{2}}$ , 量化步长  $\Delta$  由水印方差  $\sigma_w^2$  和缩放因子  $\alpha$  决定. 从以上分析可知, 量化步长  $\Delta$ 、缩放因子  $\alpha$  和扩频因子  $L$  控制水印嵌入强度, 是维系作品拷贝失真与检测性能的支点, 它们在混合模型中存在最优值, 在实验部分将进一步进行阐述.

由于多小波具有短紧支、正交、对称、高消失矩的性质, 载体信号在多小波变换下的细节子带具有很好的分布特征, 图

4(b) 分别是“Lena”图像两层多小波分解三个细节子带 (LH、HL 和 HH) 的统计分布图, 可以看出分布近似服从均值为零的高斯分布. 由于在高斯分布下的相关检测是最优检测器, 混合水印算法公式 (6) 中相关系数也可看作是归一化相关检测, 多小波变换的这种性质有利于提高检测器性能.

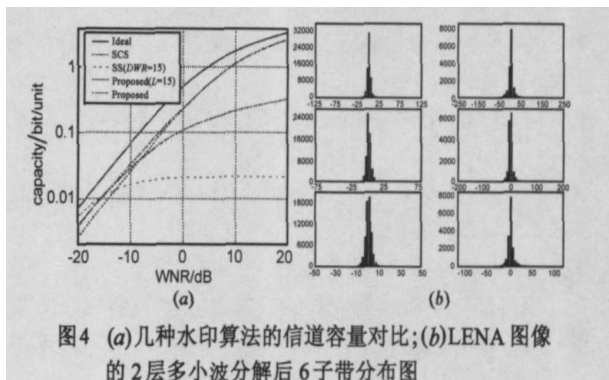


图 4 (a) 几种水印算法的信道容量对比; (b) LENA 图像的 2 层多小波分解后 6 子带分布图

## 5 试验结果及分析

本试验以“Lena”灰度图像为测试图, 在 Matlab 环境下完成程序实现, 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. 按照本文所提出算法, 实验过程分解图例如图 5 所示.

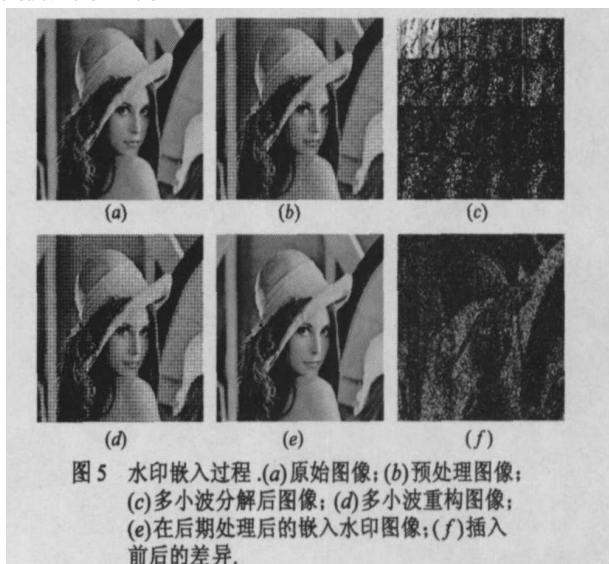


图 5 水印嵌入过程. (a) 原始图像; (b) 预处理图像; (c) 多小波分解后图像; (d) 多小波重构图像; (e) 在后期处理后的嵌入水印图像; (f) 插入前后的差异.

在所提算法中, 影响算法性能的参数有: 缩放因子  $\alpha$ 、量化步长  $\Delta$  和扩频因子  $L$ . 为了测试所提出水印算法的性能, 分别针对这三个参数以及 JPEG 压缩下的水印健壮性进行实验和分析. 由于多小波反变换重构图像的截断误差的影响, 引入了量化噪声, 因此, 与理论推导结果比较, 将其视为信道噪声, 相当于增加了  $WNR$ . 试验发现, 嵌入长度  $L = 128$  时, 嵌入错误概率趋于零, 即  $P_e = 0$ . 为了反映算法中主要参数对算法性能的影响, 试验主要针对  $L$  较小, 误差可以观察的范围内进行, 即  $L = 128$ .

缩放因子  $\alpha$  也是一个较为重要的参数. 为了检验  $\alpha$  与图

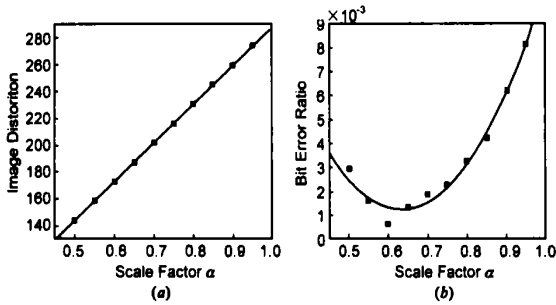


图6  $\alpha$ 对所提出水印算法的性能影响( $L=64$ ). (a)受 $\alpha$ 影响图像失真的变化; (b)受 $\alpha$ 影响BER的变化  
 像失真的影响,我们在[0.5, 1]内改变 观察图像的失真  $D_I = S - S'$ ,实验结果如图6(a)所示,可见 与图像失真成线性关系.同时,由式(5)、(7)和(8),可以将水印嵌入表示如下:  
 $X_i = X_i + q_i W_i$ ,因此 与图像失真  $D_I$  成正比,这与实验结果是一致的.关于 对比特错误率(BER)的影响,一方面,在扩频技术中 控制水印的嵌入强度;另一方面,在量化水印中 控制量化码书间距的缩放.因而,存在某个最优值  $\alpha_{opt}$ ,当  $\alpha_{opt}$ 时,可以认为增大 而带来的失真就是对水印信号能量的增强;当  $\alpha_{opt}$ 时,增大 就是对量化噪声能量的增强.这种情况如图6(b)所示,当 较小时,BER随着 的增大而减小;当 大于某个值时,BER随着 的增大而增大,并且实验发现,最优值  $\alpha_{opt} \approx 0.65$ .

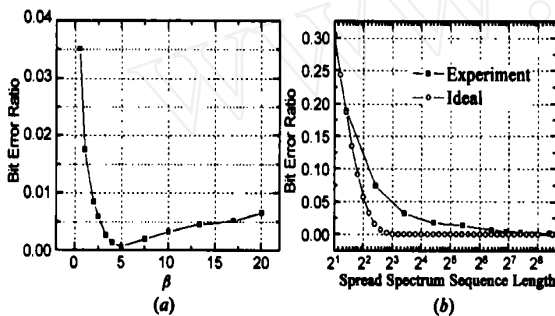


图7 强度因子 $\beta$ 和扩频长度 $L$ 对所提出水印算法的性能影响.  
 (a)受 $\beta$ 影响BER的变化;(b)在WNR=5dB和DWR=10dB下 $L$ 对BER的影响

为了考察量化步长 对算法的影响,不妨令  $\sigma_w = 0.65$ ,其中 被称为量化强度因子且  $\sigma_w > 0$ .通过选择不同的 ,来观察量化步长对错误概率的影响.当  $L = 125$ ,  $\sigma_w = 0.65$ 时 与BER之间的关系如图7(a)所示,对于某个最优值  $\beta_{opt}$ ,当  $\beta < \beta_{opt}$ 时,随着 增大BER递减;当  $\beta > \beta_{opt}$ 时,随着 增大BER递增.试验说明量化步长的增大增强了水印区分能力,但是,过大的步长又使得量化噪声迅速增大,因而增大了检测错误率.从图中估算出最优值  $\beta_{opt} \approx 5$ ,与理论量化公式  $\beta_{opt} = \sqrt{12} \cdot \sigma_w / \sigma_w = \sqrt{12} \cdot 0.65 = 5.33 \cdot \sigma_w$ 是一致的.

在理论上扩频因子  $L$  增加会减少算法的错误率(BER),同时,  $L$  的增大也会使得水印容量减少,因而,在鲁棒性和信道容量之间寻找一个平衡点是扩频因子优化的关键.当  $\sigma_w = 0.65$ ,  $\sigma_w = 5$ 时,扩频因子与BER的关系如图7(b)所示,由于多小波分解在层与层之间、子带与子带之间都存在复用关系,试验只使用一层多小波变换,水印嵌入高频部分,因此扩频因

子  $L = \log_2(4 \cdot L_e / 3)$ ,其中  $L_e$  为每比特嵌入序列长度,在图中采样点偏移了约 1.4 个单位,虽然与 WNR = 5dB 和 DWR = 10dB 情况的理想曲线比较存在误差,但已经较为接近.由试验可以看出,当  $L_e = 64$  时,错误率(BER)是可以接受的.与扩频水印(SS)扩频因子  $L_{SS}$  一般要大于 512 相比较,水印容量有较大的提高.同时,扩频因子  $L$  的减少并没有降低水印的健壮性,试验中我们发现,对于相同的实验条件,增大扩频因子水印鲁棒性增强,但是当  $L$  增大到一定程度后,鲁棒性不会继续随着  $L$  的增大而继续增强,这与扩频水印不同的,图8(a)是两层水印嵌入、水印方差  $\sigma_w^2 = 0.5$  和 1 情况下,对  $L_e = 64, 128, 256$  和 384 进行 JPEG 压缩试验的结果,水印容量分别是 2556、1920、960 和 636 比特,不难看出,  $L_e = 128$  后 JPEG 产生的错误率已经没有明显变化,同时,算法也具有较弱的鲁棒性.

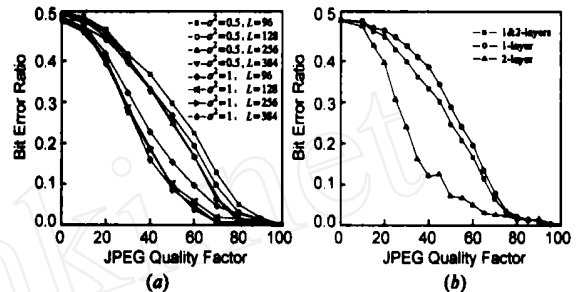


图8 (a)  $\alpha=0.65$ 和2层水印嵌入时,在不同 $L$ 、 $\sigma_w^2$ 及JPEG压缩下的BER变化;(b)第1层和第2层DMWT水印在JPEG压缩下的BER变化

为了测试鲁棒性,采用 Matlab 下的 JPEG 算法进行有损压缩试验,压缩率从 10% 到 100%,保持水印不可感知的前提下,算法采用两层多小波分解,并在两层的细节子带中嵌入水印,在不同水印方差  $\sigma_w^2$  和扩频因子  $L$  情况下,压缩强度与错误率之间的关系如图8(a)所示,试验表明各种条件下水印具有很强的鲁棒性.为了考察多小波分解不同层的健壮性,图8(b)给出了  $L = 256$ ,  $\sigma_w = 0.65$ 、嵌入 960 比特信息情况下,多小波分解各层子带以及综合所有层的 BER 曲线,可见低频率子带比高频子带更具有鲁棒性,这是因为低频部分含有更多感知重要信息,压缩过程趋向于保留这部分信息,因此水印嵌入低频部分比高频部分具有更好的鲁棒性.压缩试验表明算法在压缩比 70% 以上具有很好的抗压缩能力.

## 6 结论

本文提出了一种基于多小波变换的扩频和量化混合水印算法,通过 Costa 模型的理论分析和试验检验,算法既具有扩频水印的鲁棒性又有相对较短的嵌入长度,并能有效地抵抗 JPEG 压缩.特别是对算法检测错误率、水印容量的分析和对比,以及嵌入强度、量化步长和扩频因子等参数的分析和试验,为了解和优化性能以及今后的研究工作奠定了基础,对其它研究工作也具有指导意义.

## 参考文献:

[1] Max H M Costa. Writing on dirty paper[J]. IEEE Trans on Information Theory, 1983, 29(3): 438 - 441  
 [2] A S Cohen, A Lapidoth. Generalized writing on dirty paper

- [A]. In Proc of ISIT '02 [C]. Lausanne: Oxford University Press, 2002. 227 - 233.
- [3] P Moulin, J A O Sullivan. Information-theoretic analysis of information hiding[J]. IEEE Trans on Information Theory. 2003, 49(3): 563 - 593.
- [4] I J Cox, J Kilian, T Shamon, T Leighton. Secure spread spectrum watermarking for multimedia [J]. IEEE Trans on Image Processing. 1997, 6(12): 1673 - 1687.
- [5] M Barni, F Bartolini, A Piva. Improved wavelet-based watermarking through pixel-wise masking [J]. IEEE Trans on Image Processing, 2001, 10(5): 783 - 791.
- [6] B Chen, G Wornell. Provably robust digital watermarking [A]. In Proc of SPIE Multimedia Systems and Applications [C]. Boston: SPIE press, 1999. 43 - 54.
- [7] B Chen, G W Wornell. Quantization index modulation: A class of provably good methods for digital watermarking and information embedding [J]. IEEE Trans on Information Theory. 2001, 47(4): 1423 - 1443.
- [8] J Eggers, R Bauml, R Tzschoppe, B Girod. Scalar cost scheme for information embedding [J]. IEEE Trans on Signal Processing, 2003, 51(4): 1003 - 1019.
- [9] J Y Tham, L-X Shen, S L Lee, H H Tan. A general approach for analysis and application of discrete multiwavelet transforms [J]. IEEE Trans on Signal Processing. 2000, 48(2): 457 - 464.

#### 作者简介:



朱岩男, 1974 年生于黑龙江大庆, 于 2003 年与 2005 年分别获哈尔滨工程大学硕士学位与博士学位, 主要研究方向为信息安全、计算复杂性理论、密码学、数字指纹和模式识别等。  
E-mail: martinzhu @msn. com



杨永田男, 1939 年生, 1966 年毕业于北京大学无线电电子学系计算技术专业, 1966 年至 1985 年在(西安)中国航空计算技术研究所从事科研工作, 于 1980 年赴英国 Cranfield Institute of Technology 电子工程系进修学习两年, 现任哈尔滨工程大学教授、博士生导师, 主要从事计算机网络及应用、分布式计算机系统、网络与信息安全等研究。

WWW.CNKI.NET