第34卷 第23期 计 算 机 工 程 2008年12月
Vol.34 No.23 Computer Engineering December 2008
·安全技术· 文章编号：1000—3428(2008)23—0184—03 文献标识码：A 中图分类号：TN911.73

基于小波基的CDMA自适应水印算法

黄美茹，高宝建，韩亚洁
(西北大学信息科学与技术学院，西安 710127)

摘 要：提出一种以正交小波基作为扩频码的CDMA自适应水印算法。该方法通过对Haar小波基进行平移和尺度伸缩，离散化为一组多值正交码序列，用它作为CDMA扩频码，将二值水印图像扩频后，自适应嵌入在宿主图像的第三级细节子图上。理论分析与仿真结果表明，该方法可有效提高隐藏信息的容量和安全性。通过与哈达玛序列和改进gold码的仿真比较，证明多值序列作为扩频码CDMA水印的抗攻击能力优于二值序列。

关键词：正交小波基；CDMA扩频；自适应水印

CDMA Adaptive Watermarking Algorithm Based on Wavelet Basis

HUANG Mei-ru, GAO Bao-jian, HAN Ya-jie
(School of Information Science and Technology, Northwest University, Xi'an 710127)

【Abstract】 A new digital CDMA watermarking algorithm based on orthogonal wavelet basis is proposed in this paper. Harr wavelet basis is changed into a multilevel orthogonal sequence by scaling and translation, which is used to encode the binary image. Then the CDMA encoded watermark is adaptively embedded into the third level detail sub-images of DWT domain. Theoretical analysis and experimental results show that the capacity of the hidden information is raised and the security is enhanced. Compared with Hadamard sequence and improved gold sequence in the simulation, the multilevel sequence performs better than binary sequence in attack-resistance.

【Key words】 orthogonal wavelet basis; CDMA spread spectrum; adaptive watermark

1 概述

CDMA技术具有可多址复用、容量大、保密性好、抗干扰能力强、抗噪声等优点，将它用在数字水印技术中，既可以增加水印的嵌入容量，又可以增强水印鲁棒性。

现有文献中CDMA扩频码通常采用m序列、gold序列等，如Joseph 等提出采用DS-CDMA 方式用m序列对字符形式的水印进行扩频，然后将水印信息嵌入到图像DCT域[1]；Silvestre 等利用原始密钥生成二值的正交码集，对水印进行CDMA扩频，将其嵌入在DFT域[2]；文献[3]提出一种基于gold码的小波域扩频水印算法。目前这些基于CDMA扩频的水印算法都采用二值序列作为扩频码。文献[4]提出了一种自适应小波域水印算法，结合人类视觉系统的掩盖特性，自适应地调整水印嵌入强度，增强了水印的鲁棒性，但该算法的嵌入容量较小。

2 水印模型

采用CDMA技术的水印嵌入和检测过程如图1和图2所示，主要包括扩频码的生成、CDMA编码、水印自适应嵌入和水印检测等几部分。下面分别讨论各部分的实现算法。

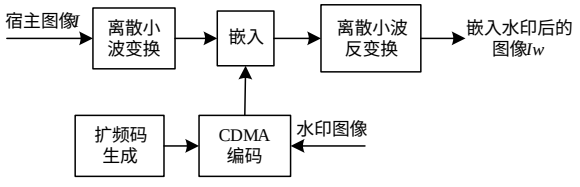


图1 水印嵌入过程

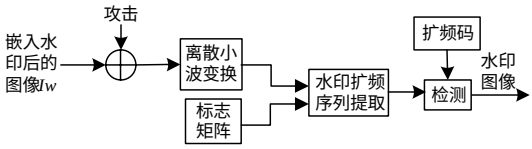


图2 水印检测过程

2.1 扩频码的生成

若一系列函数$\{e_n(x)\}$满足正交归一化条件

$$< e_i, e_j >= \delta_{ij} = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases} \quad \forall i, j \in \mathbb{Z}$$

则此函数系称为正交归一化函数系，而一个完备的正交归一化函数系称为正交归一化基。Harr小波基正是这样的一个正交归一化基，它的母尺度函数$\Phi(x)$和母小波函数$\psi(x)$[5]定义为

$$\Phi(x) = \begin{cases} 1 & 0 \le x < 1 \\ 0 & \text{otherwise} \end{cases}$$

$$\Psi(x) = \begin{cases} 1 & 0 \le x < 1/2 \\ -1 & 1/2 \le x < 1 \\ 0 & \text{otherwise} \end{cases}$$

正交规范化尺度函数和小波函数为

$$\begin{cases} \Phi_{jk}(x) = 2^{j/2}\Phi(2^j x - k) \\ \Psi_{jk}(x) = 2^{j/2}\Psi(2^j x - k) \end{cases}$$

作者简介：黄美茹(1983－)，女，硕士，主研方向：图像处理，信息安全；高宝建，副教授；韩亚洁，硕士

收稿日期：2008-04-13 **E-mail：**meiru9876@163.com

其中，j 为尺度伸缩因子；k 为平移因子。

基于以上理论，本文选择j=0~6, k=1~2^j，构造了 128 个长为 128 的小波基序列，从中选取 32 条码序列作为CDMA扩频码，记为矩阵$\boldsymbol{G}^{w}{}_{32\times128}$。

2.2 CDMA 编码

CDMA 编码的目的是将多个用户信号合并，并保持一定的独立性，其优越性在数字水印中体现为很强的鲁棒性。步骤如下：

(1)水印图像 W 为 32×32 的二值图像，对其进行映射操作，0→1, 1→-1，变为 $\boldsymbol{B}$ 矩阵，因其可以代替有限域的异或操作，在水印检测时很有用。

(2)CDMA编码。可得到如下向量：$\boldsymbol{S}=\boldsymbol{B}\cdot\boldsymbol{G}^{w}{}_{32\times128}$，嵌入时将其组成一行，$S_k=\{s_1,s_2,\cdots,s_{32\times128}\}$，即经过CDMA编码后的水印信息。

2.3 水印自适应嵌入过程

根据文献[4]的统计分析结果以及Weber定律[6]，迭加的水印信号能量和背景信号的幅值成正比，本文只选取细节子图 HL3 和LH3 的相同分块上绝对值较大的小波系数嵌入水印，并使其自适应于宿主图像，嵌入步骤如下：

(1)对 512×512 的宿主图像I进行三级小波分解，并将第三级垂直方向(LH3)和水平方向(HL3)的细节系数划分为$(64/4)^2\times2=512$ 个互不重叠的大小为 4×4 的系数块。

(2)在各个块中找出绝对值较大的 8 个系数，设立和 LH3 相同大小的标志矩阵 $\boldsymbol{L}1$ 和 $\boldsymbol{L}2$，设其初始状态为 0，矩阵元素分别与 LH3 和 HL3 子带系数相对应。若元素为 0，则该位置上子带系数非较大系数，否则即为对应子带系数大小。由此生成的标志矩阵包含了水印的嵌入信息，将其保存以便后续的水印检测。

(3)用以下公式在标记出的系数上嵌入水印[4]：

$$C\_embed(x_i,y_i)=C(x_i,y_i)+\alpha\times[|C(x_i,y_i)|+\beta\times C_{LL}(x',y')]\times S_i$$

i=1, 2,⋯,32×128

其中，$C_{LL}(x',y')$为细节系数$C(x_i, y_i)$所对应的低频子图分量，代表相应位置图像的背景亮度；α和β则是水印嵌入强度的整体和局部控制因子。

公式反映了水印嵌入强度与背景亮度及纹理强弱成正比，这样符合人类视觉系统的掩盖特性。本实验中α=0.004, β=0.43。

(4)对嵌入水印的细节子图和其他子图进行三级小波重构，得到嵌入后图像 Iw。

2.4 水印检测和提取过程

水印的检测不需要原始图像，只需要标志矩阵和密钥。所传标志矩阵数据量为原始图像的 1/32，与明检测相比，要传输的数据量大大减小。

首先对水印化图像Iw进行DWT变换，通过标志矩阵$\boldsymbol{L}1$和$\boldsymbol{L}2$从相应子带中提取出行向量并将其转换为矩阵$\boldsymbol{S}'_{32\times128}$；然后利用嵌入时的密钥生成与发送端相同的扩频码序列$\boldsymbol{G}^{w}{}_{32\times128}$，再计算每个序列与CDMA序列的互相关函数。并按以下公式来检测水印比特：

$$b_{k,i}'=\begin{cases}+1 & \eta_{k,i}>0\\ -1 & \text{otherwise}\end{cases}$$

其中，$\boldsymbol{\eta}=\frac{1}{N}(\boldsymbol{S}'\cdot\boldsymbol{G}^{\mathrm{T}})$；$b'_{k,i}$为检测到的第$k$个用户的第$i$个水印比特；$\boldsymbol{\eta}$为归一化检测矩阵；$N$为扩频码长。

为验证以上提取算法的正确性，证明如下：

$$\boldsymbol{\eta}=\frac{1}{N}(\boldsymbol{S}'\cdot\boldsymbol{G}^{\mathrm{T}})=\frac{1}{N}(C\_embed(x_i,y_i)-C(x_i,y_i))\cdot\boldsymbol{G}^{\mathrm{T}}=$$
$$\frac{1}{N}\times\alpha\times[|C(x_i,y_i)|+\beta\times C_{LL}(x',y')]\cdot\boldsymbol{B}\cdot\boldsymbol{G}\cdot\boldsymbol{G}^{\mathrm{T}}=$$
$$\frac{1}{N}\times\alpha\times[|C(x_i,y_i)|+\beta\times C_{LL}(x',y')]\cdot\boldsymbol{B}$$

因为 $C_{LL}(x',y')>0$，$\alpha,\beta,N>0$，则 $\frac{1}{N}\times\alpha\times[|C(x_i,y_i)|+\beta\times C_{LL}(x',y')]>0$，所以 $\boldsymbol{B}$ 与 $\boldsymbol{\eta}$ 正负相同，若 $\boldsymbol{\eta}$>0，$\boldsymbol{B}$=+1，否则 $\boldsymbol{B}$=-1。

最后通过计算提取出的水印信号与原始水印信号之间的相关性来进行版权认证。

提取水印$W1$与原始水印W的归一化相关系数定义为[7-8]

$$NC(W,W1)=\frac{\sum_{i=1}^{L}w(i)w1(i)}{\sqrt{\sum_{i=1}^{L}w^2(i)}\sqrt{\sum_{i=1}^{L}w1^2(i)}}$$

若 $NC(W,W1)>Th$，则待测图像中含水印，否则没有水印。本文中 Th 值取为 0.5。

3 仿真结果分析

本次实验使用 512×512 的灰度图像作为原始宿主图像，水印选用 32×32 的印有“西北大学”字样的二值图像。3 种扩频码分别记为：小波基序列$\boldsymbol{G}^{w}{}_{32\times128}$，哈达玛矩阵$\boldsymbol{G}^{h}{}_{32\times128}$，改进gold码矩阵$\boldsymbol{G}^{g}{}_{32\times128}$。

哈达玛变换是以正交直角函数为基函数的正交变换，其函数系是一类只有+1 和-1 这 2 种取值的完备的正交函数系。本文中先生成 128×128 的哈达玛矩阵，然后取其中任意 32 列来生成码矩阵$\boldsymbol{G}^{h}{}_{32\times128}$。

改进gold码的生成是采用n=7 的m序列优选对(7, 6)和(7, 6, 5, 4)来生成 129 个长度为 127 的gold序列集。在其中挑选出 32 条平衡码序列，在其末尾加一个“0”，构成生成码矩阵$\boldsymbol{G}^{g}{}_{32\times128}$。

为验证本文的有效性，以下将本文方法中的生成码矩阵$\boldsymbol{G}^{w}{}_{32\times128}$替换为哈达玛矩阵$\boldsymbol{G}^{h}{}_{32\times128}$和改进gold码矩阵$\boldsymbol{G}^{g}{}_{32\times128}$分别进行比较。实验比较中用了多幅图像进行测试，但限于篇幅，这里仅列举出Lena宿主图像的比较结果。

(1)不可见性测试

从图 3 可以看出，人眼难以区分 4 幅图像的不同，说明本文实现的算法是主观不可见的。

(a)宿主图像　(b)嵌入后图像(小波基)

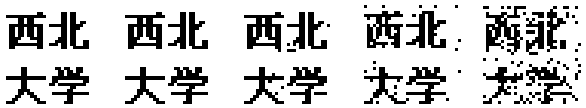
(c)嵌入后图像(哈达玛)　(d)嵌入后图像(gold 码)

图 3　水印不可见性测试

当扩频码为$\boldsymbol{G}^{w}{}_{32\times128}$时，嵌入水印后图像的*PSNR*=45.506，提取水印与原始水印间的*NC*=1；当扩频码为$\boldsymbol{G}^{h}{}_{32\times128}$时，*PSNR*=45.365，*NC*=1；当扩频码为$\boldsymbol{G}^{g}{}_{32\times128}$时，*PSNR*=45.52，*NC*=1。

(2)鲁棒性测试(仅列举出小波基算法的测试结果)

从图 4 和表 1 可以看出，在相同压缩率情况下，本文采用多值正交小波基作为扩频码方法最优。



(a)水印原图 (b)*Q*=40 (c)*Q*=20 (d)*Q*=15 (e)*Q*=10

图 4　JPEG 压缩后提取到的水印图像

表 1　JPEG 压缩性能比较

算法	*Q*=10	*Q*=20	*Q*=30	*Q*=40	*Q*=50	*Q*=60	*Q*=70	*Q*=80	*Q*=90
哈达玛	0.897 3	0.986 7	0.998 0	1.000 0	1.000 0	1.000 0	1.000 0	1.000 0	1.000 0
gold 码	0.883 2	0.977 9	0.998 0	0.998 7	0.999 3	0.999 3	1.000.0	1.000 0	1.000 0
小波基	0.900 8	0.992 0	0.999 3	1.000 0	1.000 0	1.000 0	1.000 0	1.000 0	1.000 0

从图 5 和表 2 可以看出：采用 3 种扩频码在嵌入比特数相同(32×32 的二值图像)情况下，嵌入水印后，图像质量相近；嵌入后图像在遭受相同攻击后，采用小波基的算法具有更高的 NC 值。通过对这 3 种码的比较，分析如下：小波基序列和哈达玛是严格正交的，而改进 gold 码是准正交的，因此哈达玛和小波基序列效果优于改进 gold 码 .哈达玛是二值正交，小波基序列是多值正交，效果优于哈达玛。正好相似于文献[9]所述，多值混沌序列的抗截获和抗攻击能力要强于二值序列。

(a)中值滤波(3×3) (b)维纳滤波(3×3) (c)高斯加噪

(d)椒盐加噪 (e)比例缩放 (f)剪切(25%)

图 5　常见的图像处理及几何攻击后提取水印组图

表 2　对水印图像进行各种常见攻击的性能测试比较

攻击类型	相关系数 *NC*		
	小波算法	哈达玛算法	gold 算法
JPEG 压缩(10%)	0.900 8	0.897 3	0.883 2
中值滤波 3×3	0.995 3	0.997 3	0.995 3
中值滤波 5×5	0.920 6	0.862 3	0.854 7
维纳滤波 3×3	1.000 0	0.998 0	0.999 3
维纳滤波 5×5	0.957 6	0.927 1	0.920 4
高斯加噪(0,0.01)	0.870 5	0.846 5	0.827 1
椒盐加噪(0.02)	0.908 0	0.894 4	0.880 1
比例缩放(25%)	0.848 7	0.792 7	0.800 3
剪切(25%)	0.921 7	0.783 8	0.796 4

4　结束语

本文探讨了利用正交小波基生成的多值正交序列作为 CDMA 扩频码的一种新的水印结构方法。该方法在小波域嵌入经过扩频编码的水印信息，不仅具有良好的安全性，而且比传统的基于二值正交序列的扩频水印具有更好的鲁棒性，可以为扩频水印的深入研究提供重要参考。

参考文献

[1] Joseph J K, Dowling W J. Rotation, Scale and Translation Invariant Spread Spectrum Digital Image Watermarking[J]. Signal Processing, 1998, 66(3): 303-317.

[2] Silvestre G C M, Dowling W J. Embedding Data in Digital Images Using CDMA Techniques[C]//Proc. of 2000 IEEE International Conference on Image Processing. Vancouver, Canada: [s. n.], 2000: 589-592.

[3] 方艳梅, 黄继武. 基于 CDMA 扩频技术的图像水印算法[J]. 中国图像图形学报, 2003, 8(11): 1314-1319.

[4] 朱兴力, 张家树. 基于小波系数块能量分析的自适应数字水印算法[J]. 计算机应用, 2006, 26(4): 830-832.

[5] Mallat S G. A Theory for Multiresolution Signal Decomposition: The Wavelet Representation[J]. IEEE on PAMI, 1989, 11(7): 575-593.

[6] Gonzalez C, Wintz P. Digital Image Processing[M]. 2nd ed. New York, USA: Addison-Wesley Publishing Co., 1987.

[7] Cox I J, Kil I J, Leighton F T, et al. Secure Spread Spectrum Watermarking for Multimedia[J]. IEEE Trans. on Image Processing, 1997, 6(12): 1673-1687.

[8] 李旭东. 基于分块 DCT 和量化的图像盲水印算法[J]. 计算机工程, 2006, 32(19): 167-169.

[9] Yang Tao, Chua L O. Chaotic CDMA Communication Systems[J]. International Journal of Bifurcation and Chaos, 1997, 7(12): 2789-2905.

（上接第 166 页）

表 1　资产风险

资产	资产价值	威胁事件	威胁行为发生的可能性	脆弱性程度	风险值
A	0.62	SYNFLOOD 攻击	0.87	0.90	0.44
		Land 攻击	0.79	0.69	0.31
B	0.49	Land 攻击	0.79	0.69	0.18

5　结束语

在系统地分析信息安全风险评估计算模型和系统模型的基础上，本文提出了一种基于免疫网络的风险定量评估的方法。从实验结果可以看出，本文的模型能够实时检测系统面临的威胁，较精确地评估威胁，评估出的风险值较好地反映了威胁强度的变化，具有一定的实用意义。

参考文献

[1] Alberts C J, Dorofee A J. OCTAVESM Method Implementation Guide(v2.0)[D]. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2001.

[2] Visintine V. An Introduction to Information Risk Assessment[Z]. SANS Institute, 2003-08.

[3] 中华人民共和国国家标准. GB/T 20984-2007 信息安全风险评估规范[S]. 2007.

[4] Timmis J, Neal M. A Resource Limited Artificial Immune System for Data Analysis[J]. Knowledge Based Systems, 2001, 14(3/4): 121.

[5] Nunes de C, von Zuben F J. An Evolutionary Immune Network for Data Clustering[C]//Proceedings of the 6th Brazilian Symposium on Neural Network. Rio de Janeiro, Brazil: [s. n.], 2000: 84-89.