基于 Baker 变换的自适应正交多小波图像水印算法

李会方,朱 波,徐瑞萍,马建仓
LI Hui-fang,ZHU Bo,XU Rui-ping,MA Jian-cang

西北工业大学 电子信息学院,西安 710072
School of Electronics Information,Northwestern Polytechnical University,Xi'an 710072,China
E-mail:lhuifang@nwpu.edu.cn

LI Hui-fang,ZHU Bo,XU Rui-ping,et al.Adaptive watermarking algorithm based multiwavelet transform and Baker transformation.Computer Engineering and Applications,2008,44(5):109-111.

Abstract: In this paper,an adaptive watermarking algorithm based on the discrete multiwavelet transform and the human visual perception characteristics is proposed.In this algorithm,the Bakers' transformation is used to encrypt watermark image and utilizes the visual masking in multiwavelet domain to embed the encrypted watermark in different image parts with different intensity.Experimental results show that the algorithm can improve the robust of watermarking and keep it invisible and stand against several attacks,such as filtering,scaling,cropping image,rotation and JPEG compression,also can be helpful to protect the copyright of digital images.
Key words: digital watermark;multiwavelet transform;HVS;Baker transformation

摘 要: 提出了一种基于 Baker 变换加密技术的多小波域自适应图像水印算法,充分利用了多小波变换、混沌序列的优点和人眼的视觉特性,使嵌入的水印具有很好的鲁棒性和很强的隐蔽性。实验证明该算法具有很好的抗剪切、滤波、旋转和 JPEG 压缩等优良性能。较好地解决了水印透明性与鲁棒性之间的矛盾。
关键词: 数字水印;多小波变换;人眼视觉系统;Baker 变换
文章编号: 1002-8331(2008)05-0109-03 **文献标识码:** A **中图分类号:** TP915.1

1 引言

近年来,随着多媒体产品版权保护问题的日益突出。数字水印技术引起了人们的高度重视,通常的数字水印算法包含水印嵌入和水印检测这两个基本方面。从算法的种类看,水印算法基本上分为两大类:一类方法是将数字水印按某种算法直接叠加到图像的空间域, 另一类方法是先将图像做某种变换,然后把水印嵌入到图像的变换域。变换域方法通常都具有很好的鲁棒性,对图像压缩、滤波以及噪声污染均有一定的抵抗力[1]。但是空间域方法的优点是其算法简单,计算速度比较快,但鲁棒性相对较差。从目前的情况看,变换域算法正变得日益普遍;其中尤以离散余弦变换和离散小波变换应用最为广泛。

本文主要针对正交多小波域的变换特点,提出了基于多小波变换和 Baker 变换的自适应图像水印算法。算法选取二值图像作为水印,给出了一种基于人眼视觉系统特性(HVS)的自适应水印嵌入方法。

2 数字图像的多小波分解

2.1 正交多小波变换

多小波的基本思想是将单小波中由单个尺度函数生成的多分辨分析空间,扩展为由多个尺度函数生成,以此来获得更大的自由度。因而,多小波与单小波的区别在于多小波基由多个小波母函数经过伸缩平移生成,相应地有多个尺度函数。

设 $\boldsymbol{\Phi}(x)=[\varphi_0(x),\varphi_1(x),\cdots,\varphi_{r-1}(x)]^{\mathrm{T}}$,$r\in N$,$\varphi_i\in L^2(R)$,$i=0,1,2,\cdots,r-1$,这里称满足下列条件的 $L^2(R)$ 中的子空间 $\{V_k\}_{k\in Z}$ 及函数 $\Phi(x)$ 为一个多分辨分析:

(1)$V_j\subseteq V_{j+1}$,$j\in \mathrm{Z}$;

(2)$\bigcup\limits_{j=-\infty}^{\infty} V_j=L_2(R)$,$\bigcap\limits_{j=-\infty}^{\infty} V_j=\{0\}$;

(3)存在一个函数向量 $\boldsymbol{\Phi}$ 使得$\{2^{\frac{j}{2}}\varphi_i(2^j x-k)$;$i=0,1,2,\cdots,r-1,k\in Z\}$形成 V_j 的正交规范基。

$\boldsymbol{\Phi}(x)$为多尺度函数,并且满足以下两尺度方程:

$$\boldsymbol{\Phi}(x)=2\sum_{k\in Z}\boldsymbol{h}_k\boldsymbol{\Phi}(2x-k) \tag{1}$$

同时存在一个函数向量 $\boldsymbol{\psi}(x)=[\psi_0(x),\psi_1(x),\cdots,\psi_{r-1}(x)]^{\mathrm{T}}$ 使得$\{2^{\frac{j}{2}}\psi_i(2^j x-k)$;$i=0,1,2,\cdots,r-1,k\in Z\}$形成 W_j 的正交规范基。使得 W_j 是 V_j 在 V_{j+1} 中的正交补,并且满足两尺度方程:

基金项目: 国家自然科学基金(the National Natural Science Foundation of China under Grant No.60672184)。
作者简介: 李会方(1962-),男,博士,副教授,主要研究方向为智能信号处理、多媒体信息处理和计算机应用;朱波(1980-),男,硕士研究生,主要研究方向为数字图像处理与信息隐藏技术;徐瑞萍(1962-),女,工程师,主要研究方向为电子技术与计算机应用。
收稿日期: 2007-06-18 **修回日期:** 2007-11-02

$$\boldsymbol{\psi}(x)=2\sum_{k=0}^{N-1}\boldsymbol{g}_k\boldsymbol{\Phi}(2x-k) \quad (2)$$

其中，$\boldsymbol{h}_k$ 和 $\boldsymbol{g}_k$ 均为 $r\times r$ 的常数矩阵。从信号处理的角度看，两者应该是与尺度函数和小波函数对应的 $r\times r$ 的矢量滤波器。

如果$\{\varphi_l(x-k),l=0,1,\cdots,r-1\}$构成 V_0 的规范正交基，则$\{2^{\frac{j}{2}}\varphi_i(2^jx-k);i=0,1,2,\cdots,r-1,k\in Z\}$构成 V_i 的规范正交基，称 $\boldsymbol{\Phi}(x)$为正交多尺度函数；如果$\{\psi_l(x),l=0,1,\cdots,r-1\}$构成 W_0 的规范正交基，则$\{2^{\frac{j}{2}}\psi_i(2^jx-k);i=0,1,2,\cdots,r-1,k\in Z\}$构成 W_i 的规范正交基。称 $\boldsymbol{\psi}(x)$为 $\boldsymbol{\Phi}(x)$对应的正交多小波函数。

对于 $\forall f(x)\in V_0$，可分解为：

$$f(t)=\sum_{k\in Z}\boldsymbol{C}_{0,k}^{\mathrm{T}}\Phi(t-k)=\sum_{k\in Z}\boldsymbol{C}_{J_0,k}^{\mathrm{T}}2^{\frac{J_0}{2}}\Phi(2^{J_0}t-k)+\sum_{J_0\leqslant j<0}\sum_{k\in Z}\boldsymbol{D}_{j,k}^{\mathrm{T}}2^{\frac{j}{2}}\psi(2^jt-k)$$

其中 $\boldsymbol{C}_{j,k}=[c_{j,k}^{(0)},c_{j,k}^{(1)},\cdots,c_{j,k}^{(r-1)}]^{\mathrm{T}}$，$\boldsymbol{D}_{j,k}=[d_{j,k}^{(0)},d_{j,k}^{(1)},\cdots,d_{j,k}^{(r-1)}]^{\mathrm{T}}$。

将正交单小波中分析与合成的 Mallat 算法推广至正交多小波，可以得到分析过程：

$$\boldsymbol{C}_{j-1,k}=\frac{1}{\sqrt{2}}\sum_{n=0}^{N-1}\boldsymbol{h}_n\boldsymbol{C}_{j,2k+n},\boldsymbol{D}_{j-1,k}=\frac{1}{\sqrt{2}}\sum_{n=0}^{N-1}\boldsymbol{g}_n\boldsymbol{C}_{j,2k+n}\quad j,k\in Z \quad (3)$$

合成过程：

$$\boldsymbol{C}_{j,n}=\frac{1}{\sqrt{2}}\left[\sum_k\boldsymbol{h}_{n+2k}^{\mathrm{T}}\boldsymbol{C}_{j-1,k}+\sum_k\boldsymbol{h}_{n+2k}^{\mathrm{T}}\boldsymbol{D}_{j-1,k}\right] \quad (4)$$

2.2 图像的多小波分解

在离散单小波中，可直接使用 Mallat 快速分解算法进行离散小波变换。而在多小波变换时，只有矢量序列才能进行多小波变换[2]。因此，普通的离散信号（标量序列）必须经过预处理才能进行多小波变换。多小波的预处理方法主要分为两类：采用预滤波法和采用平衡多小波，其主要任务是把原始数据分裂为 r 维数据，并保持或改善多小波滤波器的性能。本文采用的是基于 Miler 等提出的自适应算法[2]。

一幅 $N\times M$ 的图像 $f(n,m)$，其中 $0\leqslant n\leqslant N-1,0\leqslant m\leqslant M-1$，若对其进行多小波变换（分解），则先要把 $f(n,m)$转化为矢量图像 $\boldsymbol{g}(n,m)$。按下面的公式把 $f(n,m)$转化为 $\boldsymbol{g}(n,m)$：

$$\boldsymbol{g}(n,m)=\begin{bmatrix}\dfrac{\varphi^{(2)}(\frac{3}{2})}{\varphi^{(1)}(\frac{1}{2})\varphi^{(2)}(1)}f(2n,m)+\dfrac{1}{\varphi^{(1)}(\frac{1}{2})}f(2n+1,m)-\dfrac{\varphi^{(2)}(\frac{1}{2})}{\varphi^{(1)}(\frac{1}{2})\varphi^{(2)}(1)}f(2n,m+1)\\ \dfrac{1}{\varphi^{(2)}(1)}f(2n,m+1)\end{bmatrix} \quad (5)$$

这种方法是先把 $f(n,m)$相邻的二行看成是某个连续信号的抽样，其中第一行看成是信号在整数点上的抽样，第二行看成是信号在半整数点上的抽样，然后按照如下的预处理公式：

$$\begin{aligned}f(x)=&\sum_{n=-\infty}^{+\infty}(f(\cdot),\varphi^{(1)}(.-n))\varphi^{(1)}(x-n)+\\&\sum_{n=-\infty}^{+\infty}(f(\cdot),\varphi^{(2)}(.-n))\varphi^{(2)}(x-n)=\\&\sum_{n=-\infty}^{+\infty}c_{0,n,1}\varphi^{(1)}(x-n)+\sum_{n=-\infty}^{+\infty}c_{0,n,2}\varphi^{(2)}(x-n)\end{aligned} \quad (6)$$

转化为 $g(n,m)$的一行，这样得到的 $g(n,m)$是一幅$\frac{N}{2}\times M$ 的矢量图像，每个象素有二个分量，对 $g(n,m)$进行多小波分解，得到 4 幅$\frac{N}{4}\times\frac{N}{2}$的矢量子带图像。

3 数字水印的嵌入与提取

3.1 基于 Baker 变换的水印图像置乱加密

所谓图像置乱技术是指将一幅图像像素的空间位置重新进行排列，将原始图像变换成杂乱无章的新图像。目前已有的图像置乱方法主要适用于方阵图像，由于其加密算法和密钥没有有效的分开，所以加密算法不能公开。面包师变换是一种将连续的平面区域反复进行拉伸和折叠的变换技术[3]，是一种混沌映射，它能够产生非常奇妙的混沌现象。通过面包师变换可以将图像置乱，从而达到加密的目的。但面包师映射的定义域在连续空间中。不能直接用于图像置乱变换，考虑面包师映射独特的拉伸性、折叠性和图像像素的特点。在进行置乱时。首先对各像素行按混沌随机序列两两配对，然后对配对后的两行进行拉伸折叠操作。设图像矩阵为 $\boldsymbol{X}$，宽和高为 M 和 N，对图像矩阵 $\boldsymbol{X}(i,j)$像素，一种改进形式的面包师变换公式为：

$$p(i,j)=\begin{cases}(2i,2j-1),1\leqslant i\leqslant\frac{M}{2},1\leqslant j\leqslant\frac{N}{2}\\(2i-1,2N-2j+2),1\leqslant i\leqslant\frac{M}{2},\frac{N}{2}<j\leqslant N\\(2i-M,2j),\frac{M}{2}<i\leqslant M,1\leqslant j\leqslant\frac{N}{2}\\(2i-M-1,2N-2j+1),\frac{M}{2}<i\leqslant M,\frac{N}{2}<j\leqslant N\end{cases} \quad (7)$$

最后建立样本和次序统计量之间的对应关系$(i,j)\leftrightarrow(i',j')$，得到水印置乱后的图像：

$$\boldsymbol{X}^*=\{x_{i',j'}^*|x_{i',j'}^*=x_{i,j}|1\leqslant i,i'\leqslant m\ \text{and}\ 1\leqslant j,j'\leqslant m\} \quad (8)$$

3.2 自适应水印嵌入与提取算法

根据人眼视觉系统（HVS）的特性[4]，当嵌入水印强度低于一门限时，人眼对图像的感知质量不变，此时称嵌入的水印是不可见的。为保证水印的鲁棒性，必须使水印的强度尽量接近这一门限。因此适当地选取水印嵌入的强度因子是设计水印算法的关键。

另一方面人类视觉系统的照度掩蔽特性和纹理掩蔽特性表明，背景的亮度越亮，纹理越复杂，人类视觉对其轻微变化就越不敏感。因此，从透明性角度考虑，应尽可能地将水印嵌入到图像中满足上述条件的部位。相对应于图像的小波变换域中一些较大值的小波系数上。而从鲁棒性角度考虑，低频逼近系数集中了图像的大部分能量，是视觉上最重要的成分，适当地嵌入水印，可以保证水印的鲁棒性。所以，结合这两种情况，按照 HVS 的特性把水印图像嵌入到原始图像小波分解后的低频和中频逼近子图中。

首先利用多小波变换将原始信号图像分割成具有金字塔结构的不同频带，然后将水印信息附加在原始图像的小波系数上。加密后的水印嵌入公式如下：

$$Y'_{m,d}(i,j)=\begin{cases}Y_{m,d}(i,j)+\alpha(m,d)[T_{m,d}(i,j)]*W(i,j), & Y_{m,d}(i,j)\geqslant E_{m,d}\\ Y_{m,d}(i,j), & Y_{m,d}(i,j)<E_{m,d}\end{cases} \quad (9)$$

其中 $W(i,j)$ 为水印信息，$\alpha(m,d)$ 为第 m 级子带图像的强度因子；$T_{md}(i,j)$ 是视觉掩蔽函数，表示第 m 级第 d 个子带图像处的视觉掩蔽值；E_{md} 表示第 m 级第 d 个子带图像的能量，分别如下定义：

$$\alpha(m,d)=\begin{cases}\sqrt{2} & \text{if } d=HH\\ 1 & \text{其他}\end{cases}\left\{\begin{matrix}1.00 & \text{if}=0\\ 0.32 & \text{if}=1\\ 0.16 & \text{if}=2\\ 0.10 & \text{if}=3\end{matrix}\right\} \quad (10)$$

$$E_{m,d}=\frac{1}{N_{m,d}^{2}}\sum_{i=1}^{N}\sum_{j=1}^{N}I_{m,d}^{2}(i,j) \quad (11)$$

$$T_{m,d}(i,j)=\frac{1}{N_{m,d}^{2}}(I_{m,d}(i,j)-e_{m,LL})^{2} \quad (12)$$

其中 $N_{m,d}$ 指第 m 级第 d 子带的大小；$e_{m,LL}$ 表示第 m 级的低频子带 LL 的均值。这里，由于低频部分和中频部分是图像信号的主要部分，携带有较多的能量，而大的小波系数对应着更强的纹理，水印嵌入于此具有更好的鲁棒性，所以可以把水印信息分为对等的两半：前一半水印信息嵌入低频 LL3 子带，后一半水印信息先嵌入中频 LH3、HL3、HH3 子带，然后在冗余嵌入中频 LH2、HL2、HH2 子带。这样可既可保证水印的鲁棒性，又可使嵌入水印后图像的质量变化小。最后得到加入水印后的彩色图像 P'。

水印的提取与检测步骤如下：

第一步：把原始图像做自适应多小波分解。

第二步：计算强度因子 $\alpha_{m,d}$ 和视觉掩蔽函数 $T_{m,d}(i,j)$，然后将相应的子带做相减运算。

$$W_{m,d}(i,j)=\frac{Y'_{m,d}(i,j)-Y_{m,d}(i,j)}{\alpha_{m,d}T_{m,d}(i,j)} \quad (13)$$

第三步：对提取出的信号进行解密。

第四步：将得到的水印序列中的–1 变为 0，即可恢复出原始水印图像。

本文采用如下的峰值信噪比 $PSNR$ 的计算公式来检测嵌入水印后的效果：

$$PSNR=10\lg\left(\frac{P(x,y)_{\max}^{2}}{MSE}\right) \quad (14)$$

$$MSE=\frac{\sum_{x}\sum_{y}[P(x,y)-P'(x,y)]^{2}}{256^{2}} \quad (15)$$

其中，MSE 为均方差，$P(x,y)$ 为原图像的灰度值，$P'(x,y)$ 为重构后的图像的灰度值。

4　实验结果

为了证明算法的有效性，本文采用 256×256×8 bit 的 Lena 图像作为原始图像，水印是 32×32 的二值图像。水印进行两次面包师变换加密后进行嵌入。对 Lena 图像做 4 级多小波分解，为避免在多小波变换中出现边界效应，对原始图像进行了周期延拓。为了证明该算法的鲁棒性，本文做了抗压缩、抗滤波、抗剪切和抗旋转四种实验，原始图像和水印图像、嵌入水印图像和提取水印图像分别如图 1 和图 2 所示。从图中很难看出它与原始图像有什么区别，即此水印算法具有较好的透明性。

图 1　原始图像、水印和加密水印图像

图 2　嵌入水印的图像与提取的水印

嵌入水印的图像进行鲁棒性测试的结果如表 1、表 2、表 3 所示。表 1 表示 JPEG 压缩的水印图像相似度、峰值性噪比和压缩因数 Q 为 10%~90%提取的水印图像。表 2 表示对水印图像进行滤波后提取的水印及相似度和峰值性噪比。包括 3×3 中值滤波、5×5 中值滤波、3×3 均值滤波、5×5 均值滤波和高斯低通滤波。表 3 表示剪切水印图像左上角 1/64、剪切左上角 1/16、剪切水印图像右下角 1/64、剪切右下角 1/16、旋转 90°和旋转 180°时的水印提取结果。

表 1　JPEG 压缩的水印图像相似度和峰值性噪比

Q	Embedded	10	30	50	70	90
CR	100	62.62	78.91	94.23	96.18	98.35
$PSNR$	40.76	28.22	29.76	32.42	34.86	39.41
提取水印						

表 2　抗滤波攻击实验的结果

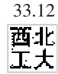
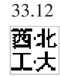
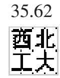
攻击方式	3×3 中值滤波	5×5 中值滤波	3×3 均值滤波	5×5 均值滤波	高斯低通滤波
CR	95.63	91.02	93.15	88.95	95.61
$PSNR$	33.12	32.02	35.62	30.11	34.78
提取水印					

表 3　抗剪切与旋转攻击实验的结果

攻击方式	左上角 1/64	左上角 1/16	右下角 1/64	右下角 1/16	旋转 90°	旋转 180°
CR	96.5	93.12	95.13	90.15	84.33	81.06
$PSNR$	33.12	36.55	35.62	32.02	28.71	30.82
提取的水印						

从以上结果可见，本文方法对于一些信号处理操作均具有较强的鲁棒性。

5　结论

本文结合混沌置乱中的 Baker 变换和人眼视觉特性，提出了一种基于面包师变换的多小波域自适应图像水印算法。该方法采用 Baker 变换对水印图像进行加密，充分利用了多小波变换、混沌序列的优点和人眼的视觉特性，使嵌入的水印具有很好的鲁棒性和很强的隐蔽性。实验证明该算法具有很好的抗剪切、滤波、旋转和 JPEG 压缩等优良性能。较好地解决了水印透明性与鲁棒性之间的矛盾，具有良好的不可见性和较高的安全性。

参考文献：

[1] Lee S J，Jung S H.A survey of watermarking techniques applied to multimedia[J].Proc IEEE ISIE，2001，1(6)：272–277.

[2] Miller J T，Li C C.Adaptive multiwavelet initialization [J].IEEE Trans SP，1998，46(12)：3282–3292.

[3] 赵雪峰.基于面包师变换的数字图像置乱[J].西北师范大学学报：自然科学版，2003，39(2)：26–29.

[4] Chou C ，Li Y C.A perceptually tuned subband image coder based on the measure of just–noticeable distortion profile[J].IEEE Trans Circuits Syst Video Technol，1995，5(6)：467–476.