基于参数小波的易碎水印安全性*

刘九芬[1,2], 黄达人[3]
(1. 中国人民解放军信息工程大学信息研究系, 河南 郑州 450002;
2. 中国科学院自动化所模式识别国家重点实验室, 北京 100080;
3. 中山大学科学计算与计算机应用系, 广东 广州 510275)

摘 要: 首先讨论所有滤波长度为 4 的双正交小波的正则性, 然后提出用这种参数小波提高易碎水印的安全性。研究结果表明: 参数小波可以很容易同现有的水印算法结合提高水印的安全性, 且不增加计算复杂度。

关键词: 参数小波; 正则性; 易碎水印; 安全性
中图分类号: TP391 文献标识码: A 文章编号: 0529-6579 (2003) 05-0011-04

在电子商务和电子政务中, 有许多电子形式的文件需要被确认。易碎水印直接在多媒体数据中嵌入有意义水印或认证符号, 通过检测嵌入水印的存在与否、真实与否以及完整与否, 确保多媒体数据的可信度。由于易碎水印可以定位篡改、承受一定的非篡改性的修改, 因此在数据完整性证明、多媒体数据认证方面具有广阔的应用前景。

由于 DWT (Discrete Wavelet Transform) 具有多分辨率特性, 使得算法可以检测到各个分辨率下篡改的特性。同时由于它的时频局部分解特性, 从而定位篡改攻击的能力强。并且 DWT 与新一代图像压缩标准 JPEG2000 兼容。因此, 研究基于 DWT 的易碎水印方案有良好的前景。但现有的基于 DWT 的水印算法都采用经典的小波, 诸如 Haar[1]、Db9/7[2] 小波等, 来分解和重构图像, 从而带来了一些安全隐患。Kundur 等[1] 指出, 若攻击者知道 DWT 域易碎水印算法的小波, 攻击者可以制造“伪认证”。

双正交小波基由于可以同时具备紧支集性、正则性和对称性, 在小波分析的理论和应用中占据了重要位置。本文首先研究所有滤波长度为 4 的双正交小波的正则性, 然后研究采用这种参数小波来提高易碎水印的安全性。

1 参数小波及正则性

为了构造双正交小波, 它对应的尺度函数 $\{\phi, \tilde{\phi}\}$ 须满足二尺度方程:

$$\phi(x) = 2\sum_{k\in\mathbf{Z}} h_k \phi(2x-k),$$
$$\tilde{\phi}(x) = 2\sum_{k\in\mathbf{Z}} \tilde{h}_k \tilde{\phi}(2x-k)$$

双正交小波由它对应的尺度函数推出, 因此双正交小波的构造归结为求 $\{h_k\}$ 和 $\{\tilde{h}_k\}$。

文献[3] 求出了所有滤波长度为 4 (即 $k\in\{0, 1, 2, 3\}$) 的双正交小波基, 和作为双正交小波基特殊情况的正交小波基。具体结论详见文献[3]。

大多数应用都要求小波有一定的光滑性, 而正则性是函数光滑程度的一种度量。并且若小波具有紧支撑, 则它的正则性和它对应的尺度函数的正则性相同[4]。因此只需讨论尺度函数的正则性。

由文献[3] 所构造的尺度函数 $\tilde{\phi}$ 的正则性由它对应的矩阵 $\boldsymbol{A}=(a_{k,l})$ 的所有特征根的模的最大值来决定[5], 其中

$$a_{k,l} = 2\sum_{n=0}^{3} h_n h_{n+l-2k} - h_{n-2k}),$$
$$k, l = -3, -2, -1, 1, 2, 3$$

通过进行复杂的计算和推导, 有如下结论:

定理 1 矩阵 $(a_{k,l})$ 的特征根的表达式如下:

$$\begin{cases} \lambda_1 = 0.5(0.5 - r_0 + \sqrt{\Delta_1}) \\ \lambda_3 = 0.5 \\ \lambda_4 = r_0 - 2r_1 \\ \lambda_5 = \lambda_6 = r_1 \\ \lambda_2 = 0.5(0.5 - r_0 - \sqrt{\Delta_1}) \end{cases} \quad (1)$$

其中, $\Delta_1 = (0.25 - 2r_0 + 4r_1)(1 - 4r_0) + r_0^2$, $r_0 =$

* 收稿日期: 2002-11-04
基金项目: 国家自然科学基金资助项目 (60172067); 国家 863 计划资助项目 (2002AA144060); 博士后基金资助项目 (2002032243)
作者简介: 刘九芬 (1963 年生), 女, 副教授; E-mail: liu_jiufen@163.net

$2(h_0h_2+h_1h_3)$, $r_1=2h_0h_3$。

由文献[3]所构造的尺度函数 ϕ 同样有定理 1 的结论，只不过 $\{h_k\}_{k=0}^{3}$ 用对应的 $\{\hbar_k\}_{k=0}^{3}$ 来代替，此时尺度函数 ϕ 对应的矩阵为 $\boldsymbol{A}=(\tilde{a}_{k,l})$。

由文献[3]及公式(1)可知，矩阵 $(a_{k,l})$ 和 $(\tilde{a}_{k,l})$ 的特征根连续。从而矩阵 $(a_{k,l})$ 和 $(\tilde{a}_{k,l})$ 特征根的模的最大值也连续。图 1 表示 $h_0=h_1=0$ 时，矩阵 $(\tilde{a}_{k,l})$ 的特征根模的最大值，此时矩阵 $(a_{k,l})$ 的特征根模的最大值为 0.5；当 $0.310\ 5\leqslant h_0\leqslant 0.5$ 时，$(\tilde{a}_{k,l})$ 的特征根模的最大值为 0.5。

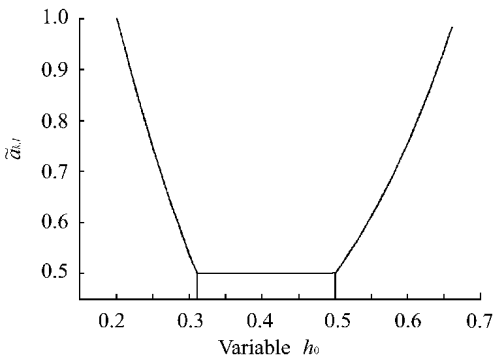

图 1 $h_0=h_1=0$，$(\tilde{a}_{k,l})$ 特征根模的最大值

Fig. 1 The largest moduli of the eigenvalues of $(\tilde{a}_{k,l})$ with $h_0=h_1=0$

图 2 表示 $h_0=h_1=0.5$ 时，矩阵 $(\tilde{a}_{k,l})$ 的特征根模的最大值，此时矩阵 $(a_{k,l})$ 的特征根模的最大值为 0.5；当 $-0.189\ 5\leqslant h_0\leqslant 0$ 时，$(\tilde{a}_{k,l})$ 的特征根模的最大值为 0.5。

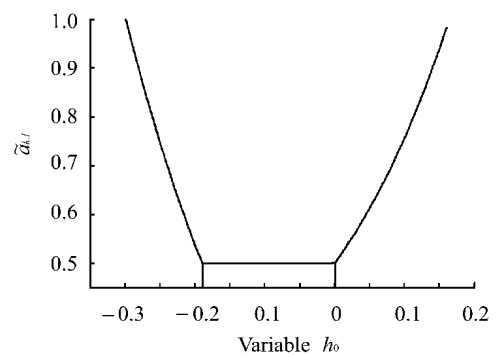

图 2 $h_0=h_1=0.5$，$(\tilde{a}_{k,l})$ 特征根模的最大值

Fig. 2 The largest moduli of the eigenvalues of $(\tilde{a}_{k,l})$ with $h_0=h_1=0.5$

图 3 表示 $h_0\neq h_1$ 时，矩阵 $(a_{k,l})$ 和 $(\tilde{a}_{k,l})$ 特征根的模的最大值的最大值图（取 1，当 h_0 和 h_1 在取值范围外）。图 4 表示当 $-\pi<t\leqslant\pi$ 时矩阵 $(a_{k,l})$ 特征根的模的最大值。它在 $[-3\pi/4,\pi/4]$ 关于 $-\pi/4$ 单调对称，在 $(-\pi,\pi)\setminus(-3\pi/4,\pi/4)$ 为 0.5。

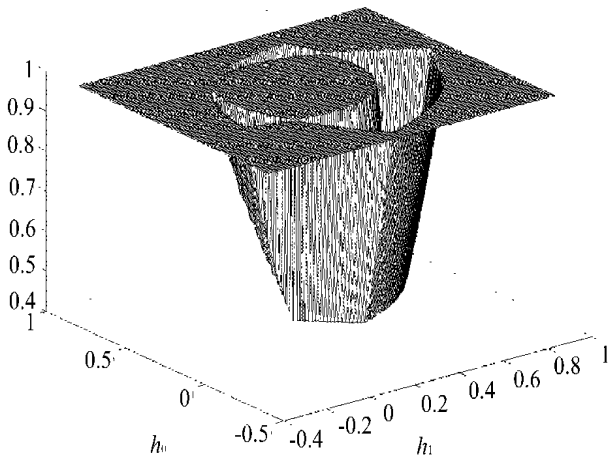

图 3 $h_0\neq h_1$，$(a_{k,l})$ 和 $(\tilde{a}_{k,l})$ 特征根模的最大值的最大值

Fig. 3 The maximum of the largest moduli of the $(a_{k,l})$ and $(\tilde{a}_{k,l})$ with $h_0\neq h_1$

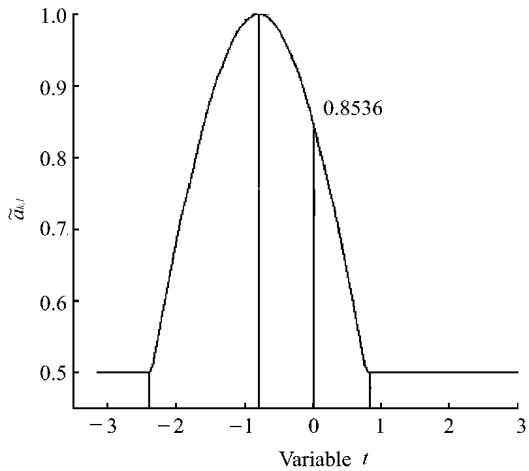

图 4 $(a_{k,l})$ 特征根模的最大值

Fig. 4 The largest moduli of the eigenvalues of $(a_{k,l})$

2 参数小波与易碎水印的安全性

2.1 易碎水印的安全性

针对易碎水印的攻击有别于稳健水印。在稳健水印中，攻击者的目的是千方百计地破坏水印或者替换水印，使得水印提取失效。易碎水印则不同，攻击者的目的在于修改图像内容而逃过水印的检测[6]。也就是说，攻击者希望以一种水印不可探测的行为来对原图像进行篡改。因此，水印机制的安全性主要在于抵抗此类攻击。

针对易碎水印的攻击主要可以分为无意的和有意的两类。无意的攻击包括压缩、信道误码等。这类攻击的产生是不可避免的，对图像的影响也不是很大。对于有意的攻击，攻击者试图发现水印的嵌入和检测机制，研究在不损害检测结果的前提下修

改图像内容的可能性；或者恢复原始水印和嵌入机制，伪造水印图像，破坏正常的系统运作。这是水印设计者有必要考虑的一种攻击。

我们用上述参数构造的小波分解原始图像。由于参数的使用导致小波滤波器是秘密的，因此水印分量嵌入到一个秘密的多分辨率变换域。若秘密参数的空间足够大，攻击者很难发现水印的嵌入和检测机制。Kundur 等[1] 指出，若小波滤波器是秘密的，制造“伪认证”是非常困难的。

2.2　参数空间

参数空间足够大吗？需要注意的问题是，参数需要离散取值。给出一维信号$\{x_m\}_{m\in\mathbf{z}}$，令 $c_m^0 = x_m$，则小波分解公式为：

$$c_k^{j-1} = \sqrt{2}\sum_l h_{l-2k}c_l^j, \quad d_k^{j-1} = \sqrt{2}\sum_l g_{l-2k}c_l^j \tag{2}$$

其中，$\sum_k h_k = 1$, $g_k = (-1)^k h_{1-k}$, $\sum_k g_k = 0$。

由文献[3] 可知，小波滤波器都是参数的连续函数。由式(2) 可知，当参数的变化比较大时，小波系数的变化也比较大；当参数的变化比较小时，小波系数的变化也比较小。因此参数必须按一定的间隔取值，才能保证它们对应的小波系数有足够的不同，才能保证不同的滤波器提取的水印信息是不同的，达到安全性的目的。

易碎水印追求针对篡改的敏感程度，使它对任何加诸于信号的变化敏感。由于各类有效攻击的直接后果就是导致图像在像素值上发生微小变动，因此，为了使此类变动在检测水印上有所反映，必须令水印所能承受的像素值最大改动比它更小。从而，对易碎水印来说，参数很小的取值间隔就可使它们对应的滤波器提取的水印信息不同。因此，参数的选取虽然有上述的问题，但由于文献[3] 构造的小波分正交和双正交 2 种，双正交中又分 3 种情况，且第 3 种情况又有 2 个自变量，以及诸参数有较大的取值范围，故参数还是有相当大的取值空间。

还需要注意一个问题，大多数应用都要求小波有一定的正则性[7]。文献[3] 所构造的小波的正则性可用式(1) 和图 1－4 表示。在实际应用中，可根据具体的问题所要求的正则性，选择参数的范围。例如，注意到 $t=\pi/4$ 时就对应 Haar 小波的尺度函数，而它对应的特征根的模的最大值为 0.5。可选取对应特征根的模的最大值等于 0.5 的参数。这时正交小波的参数取值区间为 $(-\pi, \pi)/(-3\pi/4, \pi/4)$。显然这是安全性(参数空间) 和小波分解性质的一个折衷。

3　实验和结论

实验的重点是检验易碎水印的安全性。先构造易碎水印的嵌入和检测算法。

3.1　水印嵌入

对图像进行小波分解，记小波系数为 $f(i,j)$。为了嵌入水印，需要计算

$$\Omega_{i,j} = \begin{cases} 0 & [f(i,j)] \text{ 为偶数} \\ 1 & [f(i,j)] \text{ 为奇数} \end{cases}$$

其中，$S = [\circ]$ 为地板函数。记当前嵌入的水印为 $W(i,j)$，则修改后的小波系数为：

$$f(i,j) = \begin{cases} f(i,j) & \text{if } \Omega_{i,j} = w(i,j) \\ [f(i,j)] \pm 1 & \text{if } \Omega_{i,j} \neq w(i,j) \end{cases}$$

其中选择加号还是减号依赖系数的正负性，正数为加负数为减。最后经小波逆变换得到水印图像。

3.2　水印提取

对待测图像进行小波分解，记分解后的系数为 $f'(i,j)$。提取水印为：

$$W'_{i,j} = \begin{cases} 0 & [f'(i,j)] \text{ 为偶数} \\ 1 & [f'(i,j)] \text{ 为奇数} \end{cases}$$

3.3　实验结果

我们在图像“Tiger”(1 024×1 024×8 bits，图 5) 上测试所提出的参数小波滤波器的安全性。由于滤波长度为 4 的小波中，只有 Haar 小波和 Db2 小波常用，我们首先把它们作为实验对像。

图 5　原始图像

Fig. 5　Original image

图 6　水印

Fig. 6　Watermark

图 6 是水印 (128×128×1 bits)。测试图像分解三级，水印按嵌入算法嵌入小波图像低频带。图

7 是 $t=\pi/4$ 时（对应 Haar 小波）嵌入水印，$t=\pi/4+0.005$ 提取的水印图；图 8 是 $t=5\pi/12$ 时（对应 Db2 小波）嵌入水印，$t=5\pi/12-0.01$ 提取的水印图。

图 7 提取的水印（$t=\pi/4$，Haar 小波）

Fig. 7 Extracted watermark ($t=\pi/4$, Haar wavelet)

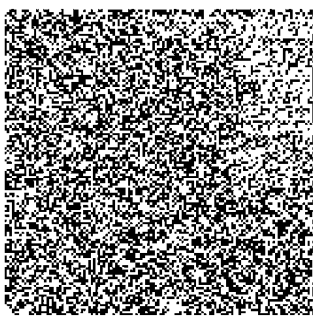

图 8 提取的水印（$t=5\pi/12$，Db2 小波）

Fig. 8 Extracted watermark ($t=5\pi/12$, Db2 wavelet)

从图 7 和 8 可以看出，提取的水印呈杂乱无章的分布，这说明用另外的参数进行水印提取不可能获得有用的信息，更谈不上非法利用这些信息。我们随后又进行了大量的实验，都有相同的结论。因此依赖参数的水印算法具有一定的安全性。

3.4 结 论

本文首先讨论了滤波长度为 4 的所有双正交小波的正则性，然后讨论了这些参数小波在易碎水印中的应用。结果表明：基于秘密参数小波滤波器的 DWT 域易碎水印算法可以提高水印的安全性。在具体的应用中，还可以依据应用所要求的正则性和具体的算法，选择参数空间。显然基于秘密滤波器的小波变换同水印的嵌入算法无关，因此现有的水印算法不用修改就可同参数小波结合起来提高水印的安全性，而且不增加算法的计算复杂度。基于秘密滤波器的小波变换是一种同嵌入算法无关的安全框架。需要说明的是，这些参数小波可用于图像、音频和视频等多媒体数据。

参考文献：

[1] KUNDUR D, HATZINAKOS D. Towards a telltale watermark technique for tamper-proofing // IEEE Int Conf on Image Processing[C]. 1998, 2: 409－413.

[2] YU G J, LU C S, LIAO Y M, et al. Mean quantization blind watermarking for image authentication // IEEE Int Conf on Image Processing[C]. 2000, III: 706－709.

[3] 刘九芬, 李峰, 黄达人. 滤波长度为 4 的双正交多尺度分析的构造[J]. 计算机学报, 2002, 25(11): 1184－1199.

[4] DAUBECHIES I. Ten lectures on wavelets. Society for Industrial and Applied Mathematics[M], Montpelier: Capital City Press, 1992.

[5] 黄达人, 刘九芬, 李峰. 滤波长度为 5 的双正交多尺度分析的构造[J]. 计算数学, 2002, 24(2): 177－188.

[6] LIN E T, DELP E J. A review of fragile image watermarks // Proc of the Multimedia and Security Workshop[C]. 1999, 25－29.

[7] MEERWALD P, UHL A. Watermark security via wavelet parametrization // IEEE Int Conf on Image Processing[C]. 2001, 3: 1027－1030.

Fragile Watermark Security Based on Parametric Wavelet

LIU Jiu-fen[1,2], *HUANG Da-ren*[3]

(1. Department of Information Research, PLA Information Engineering University, Zhengzhou 450002, China;
2. NLPR, Institute of Automation, Chinese Academy of Science, Beijing 100080, China;
3. Department of Scientific Computing and Computer Applications, Sun Yat-sen University, Guangzhou 510275, China)

Abstract: The regularity of all biorthonormal wavelets with filter length 4 is analyzed firstly. It is proposed to use secret wavelet filters to improve the security of digital watermarking schemes operating in the wavelet transform domain secondly. The results show that the parametric wavelet filters can be easily integrated into existing wavelet-based watermarking algorithms, resulting in improved security without additional computational complexity.

Key words: parametric wavelet; regularity; fragile watermarking; security