基于奇异值分解的 Contourlet 域稳健性数字水印算法*

张飞艳[a]，全桓立[a]，林立宇[b,c]，秦前清[c]
（武汉大学 a. 电子信息学院；b. 计算机学院“空天信息安全与可信计算”教育部重点实验室（B 类）；c. 测绘遥感信息工程国家重点实验室，武汉 430079）

摘 要： 提出了一种基于奇异值分解的 Contourlet 域数字水印算法。对置乱后的水印图像进行奇异值分解，在 Contourlet 域中选取合适的方向子带，利用得到的奇异值来调制系数矩阵，然后通过逆变换获取嵌入水印后的图像。在水印提取中只需要保存原始图像的奇异值，实现了水印的近似盲提取。最后，进行了一系列的攻击实验，证明了与传统小波域水印算法相比，该算法的不可见性和鲁棒性都有了较大的提高。

关键词： 数字水印；Contourlet 变换；奇异值分解；不可见性；鲁棒性
中图分类号： TP391 **文献标志码：** A **文章编号：** 1001-3695(2012)04-1402-03
doi:10.3969/j.issn.1001-3695.2012.04.056

Robust digital watermark algorithm in Contourlet domain based on singular value decomposition

ZHANG Fei-yan[a], QUAN Huan-li[a], LIN Li-yu[b,c], QIN Qian-qing[c]
(*a. School of Electronic Information, b. Key Laboratory of Space Information Security & Credibility Compute of Ministry of Education (B Class), School of Computer Science, c. State Key Laboratory for Information Engineering in Surveying, Mapping & Remote Sensing, Wuhan University, Wuhan* 430079, *China*)

Abstract: To protect the copyright of digital media, this paper proposed a digital watermark algorithm in Contourlet domain. The original image was decomposed with Contourlet transformation(CT), the scrambled watermark image was decomposed with singular value decompositino(SVD), then, the singular values of watermark image were used to modulate the chosen Contourlet coefficient matrixs. After inverse transformation, obtained a watermarked image. In watermark detection, only the SVD vector of the original image was needed, which meant the blind detection was nearly achieved. Finally, applied a series attacks, the results show that compared with traditional watermark algorithm in wavelet domain, the proposed method achieves great impovement in both invisibility and robustness.

Key words: digital watermark; Contourlet transform; singular value decompositino(SVD); invisibility; robustness

0 引言

数字水印作为一门新兴学科，在通信、计算机、密码学等领域有着广泛的应用前景，是解决信息安全、知识产权保护和认证等问题的有效方法，随着多媒体技术的日趋成熟，数字水印技术的研究也逐渐成为图像处理领域的一个热点问题[1]。

目前，图像的数字水印算法可分为空间域方法和变换域方法两大类。空间域方法通过直接对图像中的像素值进行操作，如 LSB 算法，其特点是操作简单，但是鲁棒性不足；变换域方法通过把图像变换到频域，实现频域水印的嵌入和提取，再反变换回空间域，如 DCT、DFT、DWT，其鲁棒性一般要好于前者。

水印系统应该同时满足不可见性和鲁棒性的要求，但这两者是相互矛盾的。要增强抵抗攻击的能力，就要加大嵌入强度，这就会引起图像的失真，不可见性降低；反之，减小嵌入强度，水印的鲁棒性就会降低。因此，人们提出了利用人眼视觉系统来自适应控制水印强度，在满足不可见性的条件下最大强度地嵌入水印。继小波变换之后，文献[2]提出了一种能够捕捉二维信号几何结构的新的变换方法——Contourlet 变换，通过这种变换，可以对图像进行多尺度、多方向的展开，解决了小波变换在提取方向信息上的不足。文献[3]分析了 Contourlet 系数的稀疏性和方向性优势在数字水印领域的应用，得到了很好的实验结果，但不可见性较差。文献[4]的方法将水印信号通过基于内容的乘性方案加到 Contourlet 的系数中，实现了水印的盲检测；该方法鲁棒性较好，但是实验发现，这种方法在嵌入水印后图像边缘有扭曲且对水印序列有一定要求，要使得水印嵌入前后图像的 Contourlet 系数统计分布不变。文献[5]提出的小波域奇异值算法具有较好的抗攻击性能，但不可见性较差。文献[6]提出了一种基于 HVS 的 Contourlet 变换的自适应水印算法，但其所用 HVS 模型经过实验发现效果不佳，另外在嵌入系数上没有加以选择，鲁棒性得不到保证。文献[7]将奇

收稿日期： 2011-09-23；**修回日期：** 2011-10-28 **基金项目：** 国家自然科学基金资助项目(41001256)；湖北省自然科学基金重点资助项目(2009CDA141)；空天信息安全可信计算教育部重点实验室(B 类)第一批开放研究基金资助项目

作者简介： 张飞艳(1984-)，女，博士研究生，主要研究方向为图像处理、质量评价、数字水印(fifi012@163.com)；全桓立(1988-)，男，主要研究方向为数字图像变换；林立宇(1976-)，男，副教授，博士，主要研究方向为图像压缩、超分辨率重建.

异值分解运用到空域水印嵌入算法中,实现了较好的不可见性,但鲁棒性较差。针对以上问题,本文提出了一种基于 Contourlet 变换和改进奇异值分解的数字水印算法,利用人眼视觉特性,实现了水印的自适应嵌入和盲检测。该算法能够在满足水印图像不可见性的条件下最大强度地嵌入水印信息,并且对 JPEG 压缩、JPEG2000 压缩、加噪、直方图均衡、滤波、旋转、缩放等多种攻击具有较强的鲁棒性。

1　Contourlet 变换

Do 等人提出的 Contourlet 变换也称做塔型方向滤波器组(pyramid directional filter bank,PDFB)。它是一种多分辨率、局域的、方向的影像表示方法,Contourlet 变换基的支撑区间具有随尺度而长宽比变化的"长条形结构",如图 1 所示。尺度分析和方向分析分开进行,因此对于细小的有方向的轮廓和线段的表达有着独有的优势[2]。

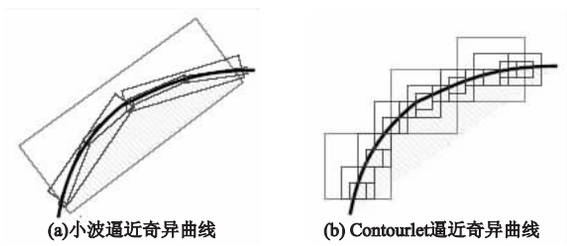


图1　奇异曲线的不同逼近方式

Contourlet 变换的实现可以看成是两个步骤:拉普拉斯金字塔(Laplacian pyramid,LP)分解和方向滤波器组(directional filter bank,DFB)滤波。合成变换过程则正好相反。将拉普拉斯金字塔和方向滤波器组进行组合,就可以构造出双迭代滤波器结构,即 Contourlet 滤波器组。图 2 显示了用 Contourlet 滤波器组对影像进行多尺度及方向分解的流程。影像的拉普拉斯金字塔分解连续地对其带通影像进行子带分解,将方向滤波器加诸于这些带通子带,便能有效地捕获方向信息。

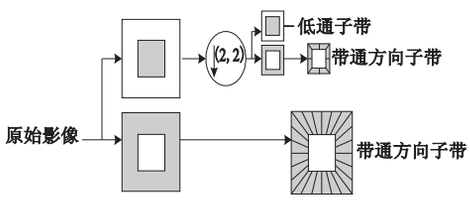


图2　Contourlet变换

2　奇异值分解

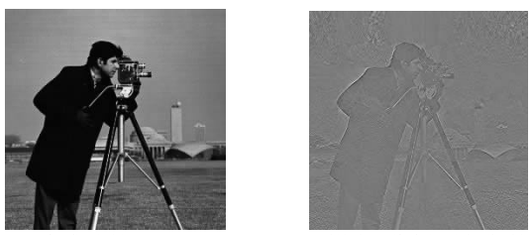
矩阵的奇异值分解定义为:设 A 为 $m \times n$ 阶实矩阵,则存在 m 阶正交矩阵 U 和 n 阶正交矩阵 V,使得

$$A = U \cdot S \cdot V^T \tag{1}$$

其中:$\mathrm{diag}(S) = (\sigma_1, \sigma_2, \sigma_3, \ldots, \sigma_k)$,$\sigma_k > 0$,记为 Λ,$k = \mathrm{rank}(A)$。S 的元素从大到小排列,在数值上呈指数递减的变化趋势,S 特征向量中的前几个分量包含了图像代数属性的主要信息。U,V 的元素 u_i,v_i 称为左右奇异值向量元素,S 的 k 个不为 0 的对角元素称为 A 的奇异值,构成了 A 的奇异值向量。

将此矩阵分析方法引入到图像处理领域可知:图像的奇异值向量可以很好地表征图像的结构信息,如图 3 所示,对一幅图像,如图 3(a)做奇异值分解,重构时,将奇异值向量替换为同样大小的单位对角矩阵,得出图 3(b)[8]。

由图 3 所示,剥除奇异值向量后,图像的结构信息几乎完全被屏蔽,由此可见,图像的奇异值向量包含了图像的绝大部分能量和结构信息,在图像处理领域引入奇异值分解概念是对图像特征提取的一大应用,这也是本文算法的理论基础。



(a) 标准测试图cameraman　　(b) 剥除奇异值向量后的残差图像

图3　奇异值对图像的表征能力

3　基于奇异值分解的 Contourlet 域数字水印算法

3.1　水印置乱

目前常见的置乱技术主要有正交变换、Gray 变换、Arnold 变换、仿射变换、幻方变换、混沌变换等方法。这些变换尽管都能达到一定的置乱效果,但存在着受图像大小变化的限制、变化数小、解密算法难以求得或解密较费时等问题[5]。针对上述问题,本文提出一种简单的随机数组置乱加密方法,该算法无须迭代,实现简单、效率较高、安全性较好,有一定的应用价值。

选择一幅 $m \times n$ 自然图像 W 作为水印,作如下置乱:

a)将水印图像表示成一个长度为 $\mathrm{len} = m \times n$ 的序列 $A\{a_i \mid 0 < a_i \leqslant 255, i \leqslant \mathrm{len}\}$。

b)初始化 $i = 1$,利用随机数发生器产生一个随机整数数列 $B\{b_i \mid 0 < b_i \leqslant \mathrm{len}, i \leqslant \mathrm{len}\}$;

c)$\mathrm{temp} \leftarrow a_i$,$a_i \leftarrow a[b_i]$,$a[b_i] \leftarrow \mathrm{temp}$;

d)$i = i + 1$;

e)若 $i \leqslant \mathrm{len}$,转 c),否则一次置乱结束;

f)初始化 $j = 1$,利用随机数发生器产生一个随机整数数列 $C\{c_j \mid 0 < c_j \leqslant \mathrm{len}, j \leqslant \mathrm{len}\}$;

g)$\mathrm{temp} \leftarrow b_i$,$b_i \leftarrow b[c_i]$,$b[c_i] \leftarrow \mathrm{temp}$;

h)$i = i + 1$;

i)二次置乱结束,将序列重排列为 $m \times n$ 的矩阵,记为 WI。

在水印置乱过程中,保留随机整数序列 B,C 作为水印提取密钥,作逆置乱,就可获得原始水印图像。如图 4 所示。

(a)原始水印图像　　(b)置乱后的水印图像

图4　水印图像的置乱

3.2　水印嵌入

水印嵌入算法步骤如下:

a)对原始图像 I 进行两层八个方向的 Contourlet 变换,获取八个方向子带系数。

b)低频子带对图像影响过大,不适于水印的嵌入,因此,选取方向子带进行水印的嵌入。

c)计算各个方向子带的能量,选取能量最大的两个子带进行合并作为待嵌入水印的系数矩阵 I_1,选取能量最小的两个子带进行合并作为待嵌入水印的系数矩阵 I_2,能量计算公式为

$$E = \frac{1}{MN} \sum_{m=1}^{M} \sum_{n=1}^{N} |d(m,n)|^2 \tag{2}$$

其中：E 为某子带总能量，M、N 分别为图像的宽度和高度，$d(m,n)$ 为图像某一元素值。

d）对 I_1、I_2 分别嵌入水印，嵌入过程如下：

（a）利用式（1）对水印图像进行奇异值分解，得到水印图像的左右奇异值矩阵 U_w、V_w，及奇异值向量 Λ_w；

（b）利用式（1）分别对 I_1、I_2 进行奇异值分解，得到其左右奇异值矩阵 U_{c1}、U_{c2}、V_{c1}、V_{c2}，及奇异值向量 Λ_{c1}、Λ_{c2}；

（c）利用式（3）修改奇异值向量 Λ_{c1}、Λ_{c2}，如下所示：

$$\Lambda_{c1}^* = \Lambda_{c1} + a_1\Lambda_w$$
$$\Lambda_{c2}^* = \Lambda_{c2} + a_2\Lambda_w \tag{3}$$

利用修改后的奇异值向量和式（1），获得嵌入水印后的系数矩阵 I_1^*、I_2^*。

e）作逆 Contourlet 变换，得到嵌入水印后的图像 I^*。

3.3 水印提取

a）对嵌入水印后的图像 I^* 进行两层八个方向的 Contourlet 变换；

b）利用与嵌入时同样的方向子带合并出 I_1^*、I_2^*，并利用式（1）分别对其进行奇异值分解，得到奇异值向量 Λ_{c1}^*、Λ_{c2}^*；

c）利用式（4），从 I_1^*、I_2^* 提取水印图像的奇异值向量：

$$\Lambda_{w1}^* = (\Lambda_{c1}^* - \Lambda_{c1})/a_1$$
$$\Lambda_{w2}^* = (\Lambda_{c2}^* - \Lambda_{c2})/a_2 \tag{4}$$

将水印的左右奇异值矩阵 U_w、V_w 及奇异值向量 Λ_{c1}^*、Λ_{c2}^*，带入式（1）重构水印图像，得到 WI_1^*、WI_2^*；

d）对 WI_1^*、WI_2^* 分别进行逆置乱，得到水印图像 W_1^*、W_2^*；

e）不同的攻击对 Contourlet 方向子带系数的影响有很大的不同，本算法中同时在两个系数矩阵中嵌入和提取水印图像，因此，可针对不同攻击。从 W_1^*、W_2^* 中选择质量较好的水印图像作为最终提取结果。

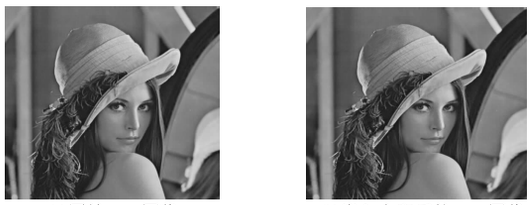
在水印嵌入和提取时，水印的置乱、Contourlet 分解级数、方向数、子带的选取都可作为密钥来保证水印的安全性，不知道这些值意味着攻击者想提取嵌入的水印是不可能的。

4 实验与分析

实验中采用一系列的（512 × 512 × 8 bit）图像（Lena、Peppers、Pirate 等）作为测试图像，采用 cameraman（256 × 256）作为水印图像，通过与文献[5]提出的水印算法的性能比较，来评估本文算法水印嵌入的不可感知性和鲁棒性。实验中，通过反复测试，并考虑到所选子带的能量差异，将式（3）中嵌入强度因子设置为：$a_1 = 0.01$，$a_2 = 0.005$。

4.1 不可感知性测试

为了评估由于嵌入水印而引起的视觉质量的下降，采用了主观视觉质量测试和峰值信噪比（PSNR）来评价本文提出的水印算法。将主观视觉质量分为五个等级，其中“5”代表“不可感知”，“4”代表“可以感知到，但不感觉讨厌”，…，“1”代表“感到非常讨厌”。峰值信噪比可以用来评估原始图像与水印图像之间的相似程度。视觉质量测试和峰值信噪比的值列于表 1。从表 1 中可以看出 PSNR 的值很大（一般在 55 dB 以上），这表明由于水印的嵌入而引起的图像质量下降很小。视觉质量测试的值一般在 4.5 ~ 5，这意味着嵌入的水印几乎是不可感知的，基本不影响主观感受。



(a)原始Lena图像 (b)嵌入水印后的Lena图像

图5 水印嵌入前后的Lena图像

表 1 视觉质量测试和峰值信噪比

灰度图像	Lena	Peppers	Pirate	Barbara	Caomei
视觉质量（本文算法）	5.0	5.0	5.0	4.75	5.0
视觉质量（文献[5]算法）	4.5	4.5	4.5	4.0	4.25
PSNR/dB（本文算法）	55.789	56.017	56.026	55.485	55.781
PSNR/dB（文献[5]算法）	41.366	41.287	41.287	41.292	41.293

4.2 鲁棒性测试

分别对水印图像做如 JPEG 压缩、JPEG2000 压缩、添加噪声处理、直方图均衡等常用图像处理方法，以及一些几何操作如随机移除、缩放、旋转等操作，提取图像水印，利用式（5）计算所提取水印和参考水印的相关系数，来评价水印算法对这些攻击的抵抗能力。矩阵 x、y 的相关系数计算公式为

$$\mathrm{NC} = \frac{E[(x - E(x)) \times (y - E(y))]}{\sqrt{E[(x - E(x))^2] \times E[(y - E(y))^2]}} \tag{5}$$

其中：NC 为 x、y 的相关系数，E 为矩阵的期望算子。

表 2 各种攻击下的水印检测结果

攻击类型	水印图像 PSNR/dB	NC 本文	NC 文献[5]	检测耗时 本文	检测耗时 文献[5]
高斯噪声 0.3	8.715	0.994	0.865	0.750	1.344
高斯滤波 5 × 5	41.558	0.988	0.875	0.781	1.257
椒盐噪 0.01	18.354	0.995	0.964	0.767	1.344
直方图均衡	16.965	0.988	0.823	0.781	1.313
Gamma 校正 0.6	6.922	0.980	0.980	0.703	0.891
Gamma 校正 1.3	6.922	0.980	0.980	0.719	0.875
JPEG（30）	25.311	0.949	0.933	0.750	1.266
JPEG2000（1:10）	36.591	0.893	0.968	0.750	1.234
缩放 0.6	29.208	0.993	0.978	0.750	1.266
缩放 1.3	39.892	0.996	0.952	0.766	1.250
缩放 3.6	41.848	0.996	0.956	0.766	1.203
随机移除 20 行 2 列	41.844	0.975	0.986	0.797	1.234
随机移除 2 行 20 列	41.658	0.974	0.934	0.719	1.297
随机移除 20 行 20 列	31.694	0.940	0.909	0.781	1.27
旋转 10°	11.167	0.990	0.958	0.906	1.344
旋转 20°	10.010	0.981	0.958	1.094	1.641

由表 2 和图 6 可知，针对图像常规攻击，如 JPEG 压缩、直方图均衡、高斯滤波和加性、乘性噪声等以及几何攻击，如图像旋转、缩放等，本文算法都可以很好地提取出水印图像，且鲁棒性优于文献[5]算法。由于文献[5]采用了小波变换，在受到同样采用小波变换的 JPEG2000 压缩的攻击时，有其固有优势，因此，本文算法略逊于文献[5]，但也能很好地提取水印图像。从相关系数及图 5 所示水印图像都可以看出，本文算法能够很好地抵抗各种攻击操作。由于选取了自然影像作为水印图像，与简单的二值水印相比，具有更强的任意性和更大的实用价值。同时，本文算法的水印嵌入和提取时间很短，基本在 0.8 s 以下，远优于文献[5]算法，具有极大的实际应用价值。

5 结束语

本文提出了不同于传统小波水印算法的 Contourlet 盲检测数字水印算法。利用 Contourlet 系数的稀疏特（下转第 1408 页）

2.1.4 解密及验证

接收方根据通信密钥,产生与发送方相同的四进制超混沌序列,与接收到的密文逐位地异或运算,即可解密,其中前 128 位为带有数据摘要的数字签名,后 L 位为明文原文。

对解密后的明文进行散列运算,形成的数据摘要与解密得到的数据摘要相同,则为正确接收。经汉字区位转换得:床前明月光,疑是地上霜。举头望明月,低头思故乡。

同时,由于混沌系统的初值敏感性,加/解密需保持严格的同步,因此通信双方还应交换相应的同步信息。

2.2 性能分析

CNN 超混沌系统结构较低维混沌系统复杂,系统的四个初始值、多个参数和采样间隔均可作为生成加密混沌序列的种子密钥,其中任一个推测错误都无法复原序列。通信成功后,服务器自动废除本次所用密钥,更新出新的密钥数据,实现“一次一密”。由于超混沌序列的随机性和复杂性,窃取者伪造密钥的可能性基本为零。混沌密钥的选取空间无限,不受密钥长度限制。密钥的生成和加/解密过程仅进行简单的数学运算,占用系统资源少,运算速度快。

基于四进制 CNN 超混沌序列生成的单向散列值,对数据的长度没有限制,无须分成固定长度的数据块;算法简单,运算速度快,可以生成任意长度的散列值;由于超混沌序列特有优越的随机性和初值敏感性,可以保护数据的完整性,防止窜改。

3 结束语

本文基于 CNN 超混沌系统分别生成了二进制和四进制超混沌序列,通过对四进制序列进行频数检验、序列检验、游程检验和相关性分析,证明了四进制混沌序列的随机性优于传统的二进制混沌序列。在此基础上,设计了一种四进制 CNN 超混沌序列在密钥的生成、加密算法和数据摘要算法中的应用方案。仿真结果表明,该方案能够实现复杂网络环境中的快速验证和加密数据传输,克服 DES、RSA、MD5 及 SHA-1 等算法已被破译的现状,具有一定的实用推广价值。

参考文献:

[1] MASUDA N, AIHARA K. Dynamical characteristics of discretized chaotic permutations[J]. International Journal of Bifurcation and Chaos, 2002, 12(10): 2087-2103.

[2] WANG Xing-yuan, WANG Xiao-juan, ZHAO Jian-feng, *et al*. Chaotic encryption algorithm based on alternant of stream cipher and block cipher[J]. Nonlinear Dynamics, 2011, 63(4): 587-597.

[3] LIU Shu-bo, SUN Jing, XU Zheng-quan, *et al*. Digital chaotic sequence generator based on coupled chaotic systems[J]. Chinese Physics B, 2009, 12(18): 5219-5227.

[4] ZHANG Yi-wei, WANG Yu-min, SHEN Xu-bang. A chaos-based image encryption algorithm using alternate structure[J]. Science in China Series F: Information Sciences, 2007, 50(3): 334-341.

[5] 王继志,王英龙,王美琴. 一类基于混沌映射构造 hash 函数方法的碰撞缺陷[J]. 物理学报,2006,55(10):5048-5054.

[6] MATFHEWS R. On the derivation of a chaotic encryption algorithm [J]. Cryptologia, 1989, 13(1): 29-42.

[7] 李孟婷,赵泽茂. 一种新的混沌伪随机序列生成方法[J]. 计算机应用研究,2011,28(1):341-344.

[8] FEI Peng, QIU Shui-sheng, MIN Long. An image encryption algorithm based on mixed chaotic dynamic systems and external keys[J]. IEEE Trans on Circuits Systems, 2005, 46(5): 1135-1139.

[9] 张雪峰,范九伦. 一种新的分段非线性混沌映射及其性能分析[J]. 物理学报,2010,59(4):2298-2304.

[10] 蒋国平,王锁萍. 细胞神经网络超混沌系统同步及其在保密通信中应用[J]. 通信学报,2000,9(2):79-85.

[11] 赵莉,张雪锋,范九伦. 一种改进的混沌序列产生方法[J]. 计算机工程与应用,2006,42(23):31-33.

[12] 张雪,马光思,毛宏燕. 基于 SSL 提高网上安全交易性能的研究[J]. 微电子学与计算机,2011,28(2):181.

[13] 王小云,张金清. MD5 报文摘要算法的各圈函数碰撞分析[J]. 计算机工程与科学,1996,18(2):15-22.

[14] TANENBAUM A S. Computer networks[M]. 4th ed. 潘爱民,译. 北京:清华大学出版社,2004:634-637.

(上接第 1404 页)

图6 各种攻击下的水印检测图像

性,选取能量最大方向子带和能量最小方向子带同时进行水印嵌入,并赋予不同的嵌入强度,利用水印图像的奇异值来进行水印图像的嵌入。在水印提取过程中,针对不同攻击类型,分别从两个系数矩阵提取水印,继而保证了水印的鲁棒性。在实验过程中,笔者发现,本文算法的嵌入和提取水印过程耗时极少,可以直接应用于在线水印检测。

参考文献:

[1] 唐笑年. 基于 BOR 多小波分解系数特点的图像数字水印技术研究[D]. 长春:吉林大学,2009.

[2] 林立宇, 张友焱,孙涛,等. Contourlet 变换——影像处理应用[M]. 北京:科学出版社, 2007: 37-42.

[3] 雍蓉,吕建平. 基于小波变换的零水印算法研究[J]. 西安邮电学院学报,2011,16(1):45-48.

[4] 李振宏,吴慧中. 基于 DWT 及方向可控金字塔变换的抗几何攻击水印[J]. 中国图象图形学报,2010,15(2):232-235.

[5] 杨俊,张贵仓,魏伟一. 基于小波变换和奇异值分解的数字水印算法[J]. 长春理工大学学报, 2005,28(4):81-84.

[6] 王员根,梁凡,肖明明. 一种彩色图像 DC 系数的自适应水印算法[J]. 中山大学学报:自然科学版,2010,31(4):146-140.

[7] 赵彦涛,李志全. 基于奇异值分解的近无损可逆数字水印方案[J]. 光电子·激光,2009,20(11):1486-1491.

[8] 朱少敏,刘建明. 基于 Contourlet 变换域的自适应量化索引调制数字图像水印算法[J]. 光学学报,2009,29(6):1523-1529.