第35卷 第20期 计 算 机 工 程 2009年10月
Vol.35 No.20 Computer Engineering October 2009
·安全技术· 文章编号：1000—3428(2009)20—0142—03 文献标识码：A 中图分类号：TP391.4

# 基于圆谐-傅里叶矩的数字水印算法

银国瑞[1,2]，平子良[1]，董佳莉[1]
(1. 内蒙古师范大学物理与电子信息学院，呼和浩特 010022；2. 武警呼和浩特指挥学院，呼和浩特 010022)

**摘 要：**针对几何攻击对数字水印的巨大破坏性，提出一种抗几何攻击水印算法，将水印信息隐藏于图像圆谐-傅里叶矩的幅度变化中。进行水印检测时只要比较受攻击图像的圆谐-傅里叶矩与密钥的差别，就能提取到水印序列。实验结果表明，该算法对旋转攻击、缩放、JPEG压缩和其他噪声攻击具有良好鲁棒性。

**关键词：**数字水印；圆谐-傅里叶矩；矩幅度；旋转和缩放攻击

# Digital Watermark Algorithm Based on Harmonic-Fourier Moment

YIN Guo-rui[1,2], PING Zi-liang[1], DONG Jia-li[1]
(1. College of Physics & Electric Information, Innermongolia Normal University, Huhhot 010022;
2. Huhhot Command College of Chinese People's Armed Police Force, Huhhot 010022)

**【Abstract】** Aiming at the serious destructiveness of geometrical attack to digital watermark, this paper proposes a geometrical attack resisted watermark algorithm. This algorithm hides the watermark information among Harmonic-Fourier moment variation of the image. The watermark sequence can be extracted by comparing the Harmonic-Fourier moment of the attacked image with the key during the watermark detection. Experimental results show that the algorithm is robustness to rotation attacks, scaling, JPEG compression and other noise attacks.

**【Key words】** digital watermark; Harmonic-Fourier moment; moment-magnitude; rotation and scaling attack

## 1 概述

数字图像水印技术是将一定信息(水印)隐藏到受保护的图像中(载体图像)构成新的图像(待检图像)，在保证水印信息不可见的前提下，当待检图像受攻击时，确保可以识别水印信息。

目前，数字水印算法主要集中在变换域和空域中[1]，文献[2]通过 Gabor 变换将数字水印信息隐藏在 DGT 的低频系数中，文献[3]通过 DCT 变换域乘嵌入水印，文献[4]通过分块量化的小波变换嵌入水印。在将空域和变换域相结合的方法中，基于不变矩的水印算法是一种抗几何攻击的有效方法。基于 Zernike 矩和伪 Zernike 矩幅度的旋转不变性，文献[5]设计了一种抗几何攻击的水印算法。与 Zernike 矩和伪 Zernike 矩相比，圆谐-傅里叶矩的图像重构能力更强，其多项式形式较简单、计算方便，重构图像时所需矩的数目较少，且矩幅度具有更好的旋转、缩放等几何不变性。因此，本文提出基于圆谐-傅里叶矩的无意义水印算法。

## 2 圆谐-傅里叶矩及其性质

### 2.1 圆谐-傅里叶矩的计算与图像重构

文献[6]提出圆谐-傅里叶矩算法，其具体思想如下：

在极坐标系 $(r,\theta)$ 中，定义函数系 $P_{nm}(r,\theta)$，包括径向函数 $T_n(r,\theta)$ 和角向函数 $\exp(jm\theta)$ 2 个部分：

$$P_{nm}(r,\theta)=T_n(r,\theta)\exp(jm\theta) \tag{1}$$

当 $n=0$ 时，$T_n(r,\theta)=\frac{1}{\sqrt{r}}$；当 $n$ 为奇数时，$T_n(r,\theta)=\frac{2}{\sqrt{r}}\sin((n+1)\pi r)$；当 $n$ 为偶数时，$T_n(r,\theta)=\frac{2}{\sqrt{r}}\sin((n+1)\pi r)$。

函数系 $P_{nm}(r,\theta)$ 在单位圆内($0\le r\le 1,\ 0\le\theta\le 2\pi$)是正交的，即

$$\int_0^{2\pi}\int_0^1 P_{nm}(r,\theta)P_{kl}^*(r,\theta)r\mathrm{d}r\mathrm{d}\theta=c\times\delta_{nmkl} \tag{2}$$

其中，$\delta_{nmkl}$ 是 Kronecker 符号；$c$ 为常数；$r$=1 为特定情形下遇到物体的最大尺寸。

极坐标系中图像函数 $f(r,\theta)$ 可以按函数系 $P_{nm}(r,\theta)$ 做正交分解：

$$f(r,\theta)=\sum_{n=0}^{\infty}\sum_{m=-\infty}^{+\infty}\Phi_{nm}T_n(r)\exp(jm\theta) \tag{3}$$

其中，

$$\Phi_{nm}=\int_0^{2\pi}\int_0^1 f(r,\theta)T_n(r)\exp(-jm\theta)r\mathrm{d}r\mathrm{d}\theta \tag{4}$$

定义 $\Phi_{nm}$ 为图像函数 $f(r,\theta)$ 的圆谐-傅里叶矩。

选取适当数量的低阶圆谐-傅里叶矩与同级次的圆谐-傅里叶函数的乘积叠加求和(式(5))，可以近似地重建原图像，选取的级次越多，近似程度越高。

$$\tilde{f}(r,\theta)\approx\sum_{n=0}^{N}\sum_{m=-M}^{M}\Phi_{nm}T(r)\exp(jm\theta) \tag{5}$$

### 2.2 圆谐-傅里叶矩的性质

#### 2.2.1 旋转不变性

设极坐标下为 $f(r,\theta)$ 的原始图像，其圆谐-傅里叶矩为 $\Phi_{nm}$，原始图像顺时针旋转 $\alpha$ 角度后的图像为 $f^r(r,\theta)$，$f^r(r,\theta)=f(r,\theta+\alpha)$，其圆谐-傅里叶矩为 $\Phi^r{}_{nm}$，则有

$$\left|\Phi_{nm}{}^r\right|=\left|\Phi_{n,m}\right|$$

**基金项目：**国家自然科学基金资助项目(60562001)
**作者简介：**银国瑞(1980－)，男，讲师、硕士研究生，主研方向：信息光学；平子良，教授、博士生导师；董佳莉，助教、硕士研究生
**收稿日期：**2009-05-11 **E-mail：**yin.guorui@163.com

2.2.2　缩放不变性

设极坐标下为 $f(r,\theta)$ 的原始图像，其圆谐-傅里叶矩为 $\Phi_{nm}=|\Phi_{n,m}|*\exp(j\beta)$，其中，$\beta$ 为 $\Phi_{nm}$ 的幅角；$|\Phi_{nm}|$ 为 $\Phi_{nm}$ 的幅度值，原始图像经过缩放后的图像为 $f^s(r,\theta)$，$f^s(r,\theta)=f(\frac{r}{k},\theta)$，其中，$k$ 为缩放倍数，其圆谐-傅里叶矩为 $\Phi^s_{n,m}=|\Phi_{n,m}{}^s|*\exp(j\beta^s)$，其中，$\beta^s$ 为 $\Phi^s{}_{nm}$ 的幅角；$|\Phi_{nm}{}^s|$ 为 $\Phi^s{}_{nm}$ 的幅度值，实验结果表明，$|\Phi_{nm}|\approx|\Phi^s_{n,m}|$。因此，圆谐-傅里叶矩的幅度具有缩放不变性。

## 3　水印算法

### 3.1　矩的筛选

先计算载体图像 $f(r,\theta)$ (Lena 图像)的 20×20 阶圆谐-傅里叶矩 $\Phi_{nm}$，并对 $\Phi_{2,2}$，$\Phi_{2,-2}$，$\Phi_{3,7}$ 和 $\Phi_{3,-7}$ 进行修改，将其幅度都扩大 10 倍，重构后的图像在一定强度下叠加到载体图像中得到待检图像，再次计算圆谐-傅里叶矩。

实验中发现，在(2, 2), (2, -2), (3, 7)和(3, -7)处，待检图像相对于载体图像的矩幅度变化量很大，而在其他位置的矩幅度变化很小。

因此，可以通过对圆谐-傅里叶矩进行修改，并将由矩的变化量组成的矢量重构水印图像，再在空域中叠加到载体图像中实现水印的嵌入。选择矩时应遵循以下原则：

(1)阶数为零的矩和重复度为 $4i$[7]，$4i$+1 和 $4i$+3($i$=0, 1, 2,…)的矩不应选为修改对象。实验中发现，上述矩在图像受到微小攻击时，其幅度会有较大变化，而重复度为 $4i$+2 矩的幅度受旋转、缩放等几何攻击的影响最小。

(2)当矩的阶数高于某一值时，计算是不准确的，不应在嵌入水印时使用。

(3)由于矩的共轭对称性，阶数相同的 2 个矩 $\Phi_{n,m}$ 和 $\Phi_{n,-m}$ 具有相同幅度值，所以，在修改其中之一的同时，必须对另一个进行相同修改，以保证水印的高质量。

### 3.2　水印嵌入的具体操作

根据以上的选取原则，水印的嵌入步骤如图 1 所示。具体步骤如下：

(1)计算载体图像 $f(r,\theta)$ 的 $N\times M$ 阶圆谐-傅里叶矩 $\Phi_{n,m}$，根据矩的选取原则，从中选取部分矩组成集合 $S$，作为预选集合。

(2)对 $S$ 中的矩进行进一步测试，选出幅度改变量受几何攻击影响较小的矩组成最优集合 $S^+$，并将其作为密钥保存，供水印检测时使用。

(3)根据要嵌入的二值水印序列 $w$，对 $S^+$中的矩进行修改，方法如下：

$\alpha_{n,m}$ 为修改系数，为了水印检测的方便，不同阶矩的幅度改变量可以通过 $\alpha_{n,m}$ 的设置来控制，即

$$|\Phi'_{n,m}|=\begin{cases}|\Phi_{n,m}|\alpha_{n,m}, & w(i)=1\\ |\Phi_{n,m}|, & w(i)=0\end{cases}$$

(4)由改变量 $\Delta_{n,m}=|\Phi'_{n,m}|-|\Phi_{n,m}|$ 组成的矩重构二值水印图像 $g(r,\theta)$。

(5)将 $g(r,\theta)$ 在一定强度下空域叠加到载体图像 $f(r,\theta)$ 中，得到待检图像 $f^{\oplus}(r,\theta)$，即 $f^{\oplus}(r,\theta)=f(r,\theta)+\beta g(r,\theta)$，其中，$\beta$ 为嵌入强度，在保证水印图像隐蔽的前提下，其值越大越好，本文中 $\beta$ =0.02。

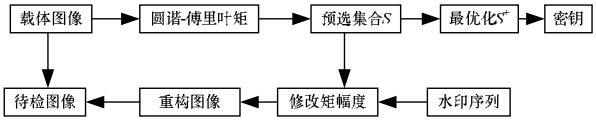


**图 1　水印嵌入图**

### 3.3　水印的检测

水印检测步骤如图 2 所示。

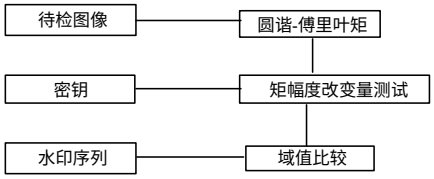


**图 2　水印检测框图**

计算待检图像的 $N\times M$ 阶圆谐-傅里叶矩，找出与密钥中相对应的各个矩，并计算出各对应矩相对于密钥的幅度变化量，设置各个矩的变化域值 $\gamma_{n,m}$，幅度变化量大于 $\gamma_{n,m}$ 的确定为水印序列的 1，小于 $\gamma_{n,m}$ 的确定为水印序列的 0，方法如下：

$$w'(i)=\begin{cases}1 & abs(|\Phi_{n,m}|-|\Phi'_{n,m}|)\geq\gamma_{n,m}\\ 0 & abs(|\Phi_{n,m}|-|\Phi'_{n,m}|)\leq\gamma_{n,m}\end{cases}$$

$\gamma_{n,m}$ 要根据修改系数 $\alpha_{n,m}$ 和嵌入强度 $\beta$ 来确定，适当的设置 $\alpha_{n,m}$ 和 $\beta$ 可以使 $\gamma_{n,m}$ 取同一值。

## 4　实验

本文采用的载体图像为 128×128 的 Lena 灰度图像(图 3)，计算矩的阶数为 $N$=40, $M$=40，嵌入强度 $\beta$ =0.02，待检图像如图 4 所示，通过 $w'(i)$ 和 $w(i)$ 的相似度来衡量水印的质量，定义 $HSD=\frac{HT(w',w)}{L}$，其中，$HT$ 表示 $w'(i)$ 和 $w(i)$ 中相同位的个数；$L$ 为水印序列的长度；$HSD$ 为水印序列的相似度。

**图 3　载体图像**

**图 4　待检图像**

为了更好地衡量水印质量与嵌入二值序列的关系，以及水印抵抗各种几何攻击的能力，本文选取不同长度的随机二值水印序列各 10 组，计算各组的实验平均值。

### 4.1　旋转攻击

将待检图像进行 0~90° 旋转，间隔为 10°，实验数据如表 1 所示。 可以看出，在嵌入水印比特值较小时，水印抵抗旋转攻击的能力较强，水印检测几乎不受旋转角度的影响，当嵌入水印比特数增加，水印的检测质量有所下降，充分验证了本文 3.2 节中的结论。

**表 1　不同角度旋转攻击下的 *HSD***

| 嵌入水印比特值 | 0° | 10° | 20° | 30° | 40° | 50° | 60° | 70° | 80° | 90° |
|---|---|---|---|---|---|---|---|---|---|---|
| 10 | 1.000 | 1.000 | 1.000 | 1.000 | 1.000 | 1.000 | 1.000 | 1.000 | 1.000 | 1.000 |
| 14 | 1.000 | 1.000 | 0.993 | 1.000 | 1.000 | 1.000 | 1.000 | 0.995 | 1.000 | 1.000 |
| 18 | 1.000 | 0.972 | 1.000 | 0.976 | 0.984 | 0.991 | 1.000 | 1.000 | 1.000 | 1.000 |
| 22 | 1.000 | 0.927 | 0.982 | 0.853 | 0.975 | 0.896 | 0.965 | 0.971 | 0.958 | 1.000 |

### 4.2 缩放攻击

对于常规的水印检测，当载体图像受到缩放攻击时，通常需要将受攻击的图像恢复到原始大小[5]，而对于本文的水印算法，由于利用了圆谐-傅里叶矩幅度的缩放不变性，水印检测时不需要将待检图像恢复到原始尺寸，直接将待检图像的矩与密钥进行比较即可。实验数据如表 2 所示，其中，$f$ 为缩放系数。当图像被放大时，*HSD* 均为 1，当图像被缩小时，由于图像的部分信息损失，因此 *HSD* 值有所下降，但都在 0.8 以上，能满足水印检测准确性的要求。

**表 2　不同比例缩放攻击下的 *HSD***

| 嵌入水印比特值 | $f$=0.5 | $f$=0.8 | $f$=1.5 | $f$=2.0 | $f$=2.5 | $f$=3.0 |
|---|---|---|---|---|---|---|
| 10 | 0.885 | 0.957 | 1.000 | 1.000 | 1.000 | 1.000 |
| 14 | 0.831 | 0.913 | 1.000 | 1.000 | 1.000 | 1.000 |

### 4.3 组合攻击

对于旋转和缩放的组合攻击，本文算法仍然具有很好的检测效果。实验数据如表 3 所示。

**表 3　不同组合攻击下的 *HSD***

| 嵌入水印比特值 | 旋转 30°+放大 1.5 倍 | 旋转 60°+放大 2 倍 | 旋转 90°+放大 3 倍 |
|---|---|---|---|
| 10 | 1.000 | 1.000 | 1.000 |
| 14 | 0.996 | 0.982 | 0.986 |

## 5　结束语

本文分析了圆谐-傅里叶矩的原理、计算、重构和性质，提出一种具有抗几何攻击性能的水印，与其他变换下的水印方法相比，本文算法具有如下优点：

(1)保密性强。将二值水印序列隐藏于圆谐-傅里叶矩的幅度变化中，水印信息不易被破译，在不了解矩的算法和密钥的情况下，即使嵌入载体图像的二值水印图像被截获，水印真实信息也不会泄露。

(2)鲁棒性强。水印信息通过变换域生成二值图像，在空域直接与载体图像叠加，结合后的载体图像是一个有机整体，水印信息不易受几何攻击的影响。

(3)水印信息提取简便。当载体图像受到几何攻击时，常规水印算法需要对载体图像进行逆向仿射变换，而本算法无须将待检图像恢复到原始尺度，极大减小了水印检测的工作量，简化了检测步骤。

图像矩修改数目的有限性限制了水印嵌入的长度，这是一个亟待解决的问题，是笔者下一步工作的重要方向。

### 参考文献


[1] 常　敏, 卢　超. 数字图像水印综述[J]. 计算机应用研究, 2003, 20(10): 1-4.

[2] 陈靖远, 陶　亮. 基于 Gabor 变换的一种有效的图像水印技术[J]. 光电子激光, 2005, 16(11): 1360-1367.

[3] 孙中伟, 冯登国. DCT 变换域乘嵌入图像水印的检测算法[J]. 软件学报, 2005, 16(10): 1798-1804.

[4] 董　敏, 王向阳. 基于分块量化的小波域数字水印嵌入算法[J]. 微电子学与计算机, 2007, 24(7): 31-34.

[5] 李雷达, 郭宝龙, 刘亚宁. 基于伪 Zernike 矩的抗几何攻击图像水印[J]. 光电子激光, 2007, 18(2): 231-235.

[6] Ren Haiping, Ping Ziliang, Wu Wenkai, et al. Multidistortion Invariant Image Recognition with the Radial Harmonic Fourier Moments[J]. J. Opt. Soc. Am. A, 2003, 20(4): 631-637.

[7] Simon X L, Pawlak M. On the Accuracy of Zernike Moments for Image Analysis[J]. IEEE Trans. on Pattern Analysis & Machine Intelligence, 1998, 20(12): 1358-1364.


编辑　陈　晖

(上接第 141 页)

$a_{12}, a_{13}, a_{14}, a_{15}, a_{16}, a_{17}, a_{18}$。为了修改 $a_{11}$ 和 $a_3$，条件 $a_0 = 0xffffffff$, $a_1 = 0$, $a_2 = 0, a_4 = 0, a_5 = 0, a_6 = 0$ 保证 $a_3$ 的改变不会影响 $a_4$, $a_5$, $a_6$, $a_7$, $a_8$, $a_9$, $a_{10}$。为了修改 $a_3$ 和 $f_0$，条件 $e_0 = 0$, $g_0 = 0$ 保证 $f_0$ 的改变不会影响 $a_1$ 和 $a_2$。

对本文算法复杂性的估计如下：

在操作 2)，从前面得到 $2^{32}$ 个 $(a_{79}, b_{79}, c_{79}, d_{79}, e_{79}, f_{79}, g_{79}, h_{79})$，从后面得到 $2^{32}$ 个 $(a_{80}, b_{80}, c_{80}, d_{80}, e_{80}, f_{80}, g_{80}, h_{80})$，一共有 $2^{64}$ 个组合，而“中间相遇”的概率是 $2^{-224}$，故需重复 $2^{160}$ 次才能得到一次“中间相遇”，由于做一次的计算量是 $2^{32}$，因此得到 224 bit 压缩值的计算量是 $2^{32} \times 2^{160} = 2^{192}$；穷举搜索其余的 32 bit 压缩值，从而算法 1 的计算量是 $2^{192} \times 2^{32} = 2^{224}$，需要存储 $2^{38}$ Byte。

## 4　结束语

过去对杂凑函数 HAVAL 安全性的分析主要集中在碰撞攻击，本文给出了对 104 步 HAVAL 压缩函数的原根攻击，该攻击表明 HAVAL 的安全性比以前认为的更弱。在实际应用中，有些环境要求杂凑函数抗原根攻击，本文的分析表明如果继续在这些环境中使用 HAVAL，会存在很大的风险。

### 参考文献


[1] Wang Xiaoyun, Lai Xuejia, Feng Dengguo, et al. Cryptanalysis for Hash Functions MD4 and RIPEMD[C]//Proc. of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques. [S. l.]: Springer-Verlag, 2005: 1-18.

[2] Wang Xiaoyun, Yu Hongbo. How to Break MD5 and Other Hash Functions[C]//Proc. of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques. [S. l.]: Springer-Verlag, 2005: 19-35.

[3] 王小云, 冯登国, 于秀源. HAVAL-128 的碰撞攻击[J]. 中国科学 E 辑: 信息科学, 2005, 35(3): 1-12.

[4] Biham E, Chen Rafi, Joux A, et al. Collisions of SHA-0 and Reduced SHA-1[C]//Proc. of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques. [S. l.]: Springer-Verlag, 2005: 36-57.

[5] Dobbertin H. The First Two Rounds of MD4 Are Not One-way[C]// Proc. of the 5th International Workshop on Fast Softwore Encrption. [S. l.]: Springer-Verlag, 1998: 284-292.

[6] Leurent G. MD4 Is Not One-way[C]//Proc. of the 15th International Workshop. [S. l.]: Springer-Verlag, 2008: 412-428.

[7] Zheng Yuliang, Pieprzyk J, Seberry J. HAVAL——A One-way Hashing Algorithm with Variable Length of Output[C]//Proc. of the Workshop on the Theory and Application of Cryptographic Techniques. [S. l.]: Springer-Verlag, 1992: 83-104.


编辑　任吉慧