一种可有效抵抗几何攻击的鲁棒图像水印算法*)

杨红颖[1] 侯丽敏[1] 王向阳[1,2]
(辽宁师范大学计算机与信息技术学院 大连 116029)[1]
(北京大学视觉与听觉信息处理国家重点实验室 北京 100871)[2]

摘 要 伪 Zernike 矩(Pesudo-Zernike Moments)是一组正交复数矩,其不仅具有旋转不变性、更低的噪声敏感性,而且还具有表达有效性、计算快速性以及多级表达性等特点。以伪 Zernike 矩理论为基础,提出了一种可有效抵抗几何攻击的数字图像水印新方案。该方案首先结合伪 Zernike 矩的旋转不变特性,计算出原始载体图像的伪 Zernike 矩;然后选取部分低阶伪 Zernike 矩;最后采纳量化调制策略将水印信息嵌入到伪 Zernike 矩幅值中。实验结果表明,该数字图像水印方案不仅具有良好的透明性,而且具有较强的抵抗常规信号处理、几何攻击等能力,整体性能优于 Zernike 矩图像水印方案。

关键词 图像水印,几何攻击,伪 Zernike 矩

Digital Image Watermarking Scheme with Pseudo-Zernike Moments

YANG Hong-ying[1] HOU Li-min[1] WANG Xiang-yang[1,2]
(School of Computer and Information Technology, Liaoning Normal University, Dalian 116029, China)[1]
(National Laboratory on Machine Perception, Peking University, Beijing 100871, China)[2]

Abstract Pseudo-Zernike moments consist of a set of orthogonal and complex number moments which have some very important properties, shch as invariantation under rotation, multilevel representation, and less sensitivity to noise. A new robust digital image watermarking scheme with pseudo-Zernike moments was proposed. Firstly, the pseudo-Zernike moments of the host image were computed. Secondly, some low-level pseudo-Zernike moments were selected. Finally, the digital watermark were embedded into the host image by quantizing the magnitudes of the selected pseudo-Zernike moments. Experimental results show that the proposed scheme is not only invisible and robust against common signals processing such as filtering, noise adding, and JPEG compression, but also robust against the some geometric attacks.

Keywords Image watermarking, Geometric attacks, Pseudo-Zernike moments

1 引言

数字水印(Digital Watermarking)作为传统加密方法的补充手段,是一种可以在开放的网络环境下保护版权和认证来源及完整性的新技术。依据应用范围,通常可以把数字水印技术划分为图像水印技术、视频水印技术和音频水印技术等。所谓数字图像水印,就是将具有特定意义的标记(水印),通过某种方法隐藏于数字图像产品中,用以证明创作者对其作品的所有权,并作为鉴定、起诉非法侵权的依据,同时通过对水印的检测和分析保证数字信息的完整可靠性,从而成为知识产权保护和数字多媒体防伪的有效手段。显然,作为数据认证和版权保护的手段,数字图像水印必然会受到各种形式的攻击,因此鲁棒性(Robustness)是数字水印系统的一项基本要求。数字图像水印技术发展到今天,已有大量不同的算法,它们广泛提出了"鲁棒性"声明。但遗憾的是,现有绝大多数图像水印方案仅仅能够对抗常规的信号处理(如有损压缩、低通滤波、噪声干扰等),而无法有效抵抗诸如旋转、缩放、平移等几何攻击。因此,抗几何攻击的高度鲁棒数字图像水印算法研究仍然是一项富有挑战性的工作[1,2]。

所谓几何攻击(Geometric Attack),并非指该种攻击能够从含水印对象中去除水印信息,而是指其能够破坏数字水印分量的同步(即改变水印嵌入位置),从而导致检测器找不到有效水印[3,4]。几何攻击包括旋转、缩放、平移、行列去除、剪切、镜像翻转、随机扭曲等多种形式。截止到目前,人们主要采用三种措施设计抗几何攻击图像水印方案,分别为构造仿射不变量[4-9]、隐藏模板[10,11]、利用图像重要特征[12]等。文献[10,11]通过在图像 DFT 中频区域嵌入模板信息的方式来估计并校正图像所经历的几何变换,从而实现水印检测的重同步,基于模板的图像水印技术具有比较好的抵抗常规处理和简单仿射变换能力,但其同样无法有效抵抗行列去除、剪切、镜像翻转、随机扭曲等几何攻击,而且水印容量受到限制。文献[12]相继提出了基于图像特征的数字水印方案,其基本思想为:利用图像中相对稳定的特征点标识水印嵌入位置,并在与每个特征点相对应的局部区域内独立地嵌入数字水印,同时利用特征点来定位和检测数字水印,从而有效抵抗几何攻击,然而目前该类方法普遍存在特征点稳定性差且分布极不

*)本文得到国家自然科学基金(60773031),计算机软件新技术国家重点实验室(南京大学)开放基金(A200702),视觉与听觉信息处理国家重点实验室(北京大学)开放基金(0503),信息安全国家重点实验室(中国科学院软件研究所)开放基金(03-06),大连市科技基金(2006J23JH020),"图像处理与图像通信"江苏省重点实验室(南京邮电大学)开放基金(ZK205014)和江苏省计算机信息处理技术重点实验室(苏州大学)开放课题基金(KJS0602)资助。

均匀等问题，严重影响了数字水印对常规信号处理的抵抗能力，同时水印容量十分有限（仅为 16bit）。相比之下，基于同步不变特征的图像水印方案以其工作原理简单、无需辅助信息、检测性能稳定等特点而受到人们重视，该类方案是从原始图像中找到具有同步不变性的量用来隐藏水印，而人们所采纳的同步不变量主要包括 Fourier-Mellin 变换、Radon 变换和几何不变矩等。在众多几何不变矩中，Zernike 矩（Zernike Moments）是一种精确的形状描述子，其不仅具有旋转不变特性，而且可任意构造高阶矩[13]，这为抗几何攻击图像水印设计提供了理论依据。Kim 等[7]通过修改低 5 阶 Zernike 矩实现了数字水印嵌入，但水印信息容量仅仅为 2bit。Chen 等[8]计算水印图像的 Zernike 矩，重构后直接嵌入到原始载体中，但其无法有效抵抗缩放和平移等攻击。Xin 等[6]首先对图像进行 Zernike 特征矢量提取，然后利用量化调制策略嵌入数字水印，同时根据提取水印的误码率（BER）判断水印存在与否，该方法可以很好地抵抗旋转和缩放攻击，但对平移攻击以及添加噪声攻击比较敏感。Farzam 等[9]首先将载体图像划分成多个同心圆，然后通过修改每个圆环的 Zernike 矩来嵌入水印信息，该方法对旋转攻击具有鲁棒性，但无法有效抵抗缩放、平移等攻击。

伪 Zernike 矩（Pesudo-Zernike Moments）[13]是一组正交复数矩，其不仅具有旋转不变性、更低的噪声敏感性，而且还具有表达有效性、计算快速性以及多级表达性等特点，故更加适合于设计抗几何攻击图像水印。本文以伪 Zernike 矩理论为基础，提出了一种可有效抵抗几何攻击的数字图像水印新方案。

2 数字水印的嵌入

本文以伪 Zernike 矩理论为基础，提出了一种可有效抵抗几何攻击的数字图像水印新方案，其基本工作原理为：首先结合伪 Zernike 矩的旋转不变特性，计算出原始载体图像的伪 Zernike 矩；然后选取部分低阶伪 Zernike 矩；最后采纳量化调制策略将水印信息嵌入到伪 Zernike 矩幅值中。

设原始载体为 256 级灰度图像 I

$I=\{f(x,y),1\leqslant x\leqslant M,1\leqslant y\leqslant N\}$

其中，$f(x,y)$表示原始载体第 x 行、第 y 列的像素灰度值，则整个数字水印的嵌入过程（关键步骤）可描述如下：

（1）水印产生。由密钥 Key1 产生一个伪随机序列 $W=\{w_i,i=1,\cdots,L\}$作为数字水印信息。其中，L 为数字水印的大小，$w_i\in\{0,1\}$。

（2）伪 Zernike 矩计算。计算原始载体图像的伪 Zernike 矩，以消除旋转攻击影响。根据正交多项式理论，Teague 等于 1979 年提出了著名的 Zernike 矩，Zernike 矩能够很容易地构造出图像的任意高阶矩，并能够使用较少的矩来重建图像。随后 Bhatia 和 Wolf 等人推导了它的正交性和不变性，并提出了伪 Zernike 矩。与 Zernike 矩相比，伪 Zernike 矩不仅具有旋转不变性、更低的噪声敏感性，而且还具有表达有效性、计算快速性以及多级表达性等特点，故可广泛应用于模式识别、图像分析等领域。

（3）选择伪 Zernike 矩。由伪 Zernike 矩相关理论知[13]：部分伪 Zernike 矩存在微小的计算误差，也就是说，必须合理选择伪 Zernike 矩用于水印嵌入。总体说来，选择伪 Zernike 矩应该考虑如下两个方面：①选择阶数较低的伪 Zernike 矩，因为当阶数高于某一数值 $M_{\max}$ 时，伪 Zernike 矩计算将不再准确。本文选取 $M_{\max}=20$；②重复度为 $n=4i(i=0,1,2,\cdots)$ 的伪 Zernike 矩存在微小计算误差，故不适合嵌入水印。显然，可用于数字水印嵌入的伪 Zernike 矩集合为

$S=\{Z_{mn},m\leqslant M_{\max},n\geqslant 0,n\neq 4i\}$

为了提高系统安全性能，我们利用密钥 Key2 从伪 Zernike 矩集合 S 中随机选择 L 个伪 Zernike 矩 $Z=(Z_{p_1q_1},\cdots,Z_{p_Lq_L})$用于水印嵌入。设其对应的伪 Zernike 矩幅值为 $A=(A_{p_1q_1},\cdots,A_{p_Lq_L})$。

（4）数字水印嵌入。本文采用量化调制伪 Zernike 矩幅值的方法实现水印信号嵌入，量化规则如下：

$$A'_{p_iq_i}=A_{p_iq_i}-DM(i)\quad(i=1,\cdots,L)$$

其中，If $w_i=1$，then

$$DM(i)=\begin{cases}\dfrac{\Delta}{2}-\delta(i),\text{if mod}(\varepsilon(i),2)=0\\ \dfrac{3\Delta}{2}-\delta(i),\text{if mod}(\varepsilon(i),2)=1, & \delta>\dfrac{\Delta}{2}\\ -\dfrac{\Delta}{2}-\delta(i),\text{if mod}(\varepsilon(i),2)=1, & \delta\leqslant\dfrac{\Delta}{2}\end{cases}$$

If $w_i=0$，then

$$DM(i)=\begin{cases}\dfrac{\Delta}{2}-\delta(i),\text{if mod}(\varepsilon(i),2)=1\\ \dfrac{3\Delta}{2}-\delta(i),\text{if mod}(\varepsilon(i),2)=0, & \delta>\dfrac{\Delta}{2}\\ -\dfrac{\Delta}{2}-\delta(i),\text{if mod}(\varepsilon(i),2)=0, & \delta\leqslant\dfrac{\Delta}{2}\end{cases}$$

这里，$\dfrac{A_{p_iq_i}}{\Delta}=\varepsilon(i)+\delta(i)$，$\Delta$ 为量化步长。

需要说明的是，量化伪 Zernike 矩幅值 $A=(A_{p_1q_1},\cdots,A_{p_Lq_L})$时，如果 $q_i\neq 0$，应同时量化它的共轭矩阵幅值 $A_{p_i,-q_i}$，以保证其具有相同幅值。

（5）含水印图像生成。结合未被修改的伪 Zernike 矩进行重构，即可得到含水印数字图像 I'。

3 数字水印的检测

本文讨论的数字图像水印检测算法属于目标检测算法，即在检测数字水印时不需要原始的载体图像。设待检测图像为 I^*，则数字水印检测过程（关键步骤）可描述如下：

（1）计算待检测图像 I^* 的伪 Zernike 矩；

（2）利用密钥 Key2 选择 L 个伪 Zernike 矩 $Z^*=(Z^*_{p_1q_1},\cdots,Z^*_{p_Lq_L})$用于水印提取。设其对应的伪 Zernike 矩幅值为 $A^*=(A^*_{p_1q_1},\cdots,A^*_{p_Lq_L})$；

（3）数字水印提取。提取规则如下：

$$\frac{A^*_{p_iq_i}}{\Delta^*}=\varepsilon^*(i)+\delta^*(i)$$

$$w_i^*=\begin{cases}0, & \text{mod}(\varepsilon^*(i),2)=1\\ 1, & \text{mod}(\varepsilon^*(i),2)=0\end{cases}$$

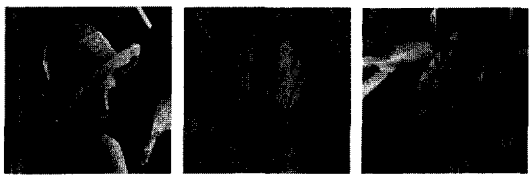
其中，Δ^* 为量化步长。

4 仿真实验结果与结论

为了验证本文数字图像水印算法的高效性，以下分别给出了透明性能测试、抗攻击能力测试的实验结果，并与文献[6]的 Zernike 矩图像水印算法进行了对比。实验中，所选用的原始载体分别为 128×128×8bit 的标准灰度图像 Lena，Baboon 和 Barbara，数字水印采用了 64bit 的二元随机序列。另外，量化步长 $\Delta=2.0$。以下在完全相同的实验环境和条件下，给出了本文算法和文献[6]算法的透明性对比（见表 1）。图 1、图 2 分别给出了本文方法及文献[6]方法的含水印图像 Lena，Baboon 和 Barbara。

表 1　含水印图像与原始载体间的峰值信噪比(dB)

图像	本文算法	文献[6]
Lena	45.43	44.367
Baboon	46.98	46.035
Barbara	45.18	44.765



(a)含水印图像 Lena (PSNR=45.43dB)　(b)含水印图像 Baboon (PSNR=46.98dB)　(c)含水印图像 Barbara (PSNR=45.18B)

图 1　数字水印的嵌入效果(本文算法)

(a)含水印图像 Lena (PSNR=44.367dB)　(b)含水印图像 Baboon (PSNR=46.035dB)　(c)含水印图像 Barbara (PSNR=44.765B)

图 2　数字水印的嵌入效果(文献[6]算法)

表 2　数字水印对常规信号处理的抵抗能力(失真率 BER)

攻击方式		失真率 BER(%)					
		Lena		Baboon		Barbara	
		本文方法	文献[6]	本文方法	文献[6]	本文方法	文献[6]
JPEG 压缩	90	0	0	0	1.56	0	0
	70	0	15.62	0	1.56	0	0
	30	5.15	15.62	1.63	9.35	1.62	4.68
高斯滤波	3*3	11.41	15.62	6.52	23.43	17.65	32.81
	5*5	18.12	53.12	13.34	45.31	27.24	45.31
高斯噪声	0.01	15.65	42.18	17.55	37.50	24.33	45.31
	0.002	11.32	53.12	11.43	50.00	11.33	29.68
椒盐噪声	0.01	9.87	51.56	19.15	28.12	7.23	20.31
	0.002	1.34	2.34	0	1.56	0	3.12

表 3　数字水印对几何攻击及联合攻击的抵抗能力(失真率 BER)

攻击方式		失真率 BER(%)					
		Lena		Baboon		Barbara	
		本文方法	文献[6]	本文方法	文献[6]	本文方法	文献[6]
旋转	5°	2.21	6.25	1.76	9.37	0	7.81
	10°	1.00	1.56	1.73	7.81	1.22	4.68
	15°	2.32	7.81	2.56	4.68	2.22	9.37
	20°	0	3.12	1.47	3.12	2.43	9.37
	25°	2.21	4.68	2.25	6.25	1.11	4.68
	30°	3.22	4.68	1.64	6.25	2.16	7.81
	90°	0	0	0	1.56	0	0
缩放	0.8	4.00	7.81	5.81	12.50	6.65	15.62
	0.9	1.16	1.56	2.12	4.68	3.12	9.37
平移(水平、垂直方向)	10	21.44	48.43	12.32	50.00	11.26	50.00
	20	13.57	43.75	13.21	51.35	10.90	59.37
	30	11.61	42.18	15.21	45.31	8.21	50.00
垂直翻转		0	0	0	0	0	0
水平翻转		0	0	0	0	0	1.56
缩放 1.2+旋转 10°		4.02	4.68	2.02	1.56	5.53	9.37
缩放 1.2+平移 10		12.42	50.00	14.61	43.75	12.43	42.18
旋转 10°+平移 20		11.65	45.31	13.45	48.43	21.64	51.56

为了检测本文算法的鲁棒性能，仿真实验分别对本文算法及文献[6]算法的含水印图像进行了一系列攻击。在完全相同的实验环境和条件下，表 2 和表 3 分别给出了本文算法和文献[6]算法的抗攻击能力对照结果(失真率 BER)。

本文以伪 Zernike 矩理论为基础，提出了一种可有效抵抗几何攻击的数字图像水印新算法，其主要特点为：(1)具有较好的抗噪声攻击能力；(2)能够有效抵抗旋转等多种形式的几何攻击；(3)算法简单、容易实现，且抽取水印时无需原始载体。其整体性能明显优于 Zernike 矩图像水印方案。

参 考 文 献

[1] Barni M, Cox I J, Kalker T. Digital watermarking//4th International Workshop, International Workshop on Digital Watermarking 2005(IWDW 2005). Siena, Italy, September 2005, Lecture Notes in Computer Science 3710, Springer, 2005

[2] Licks V, Jordan R. Geometric attacks on image watermarking system. IEEE Multimedia, 2005, 1(3): 68-78

[3] 刘九芬，黄达人，黄继武. 图像水印抗几何攻击研究综述. 电子与信息学报，2004 26(9)：1495-1503

[4] Joseph J K, Ruanaidh O, Pun T. Rotation scale and translation invariant digital image watermarking. Signal Processing, 1998, 66(3): 303-317

[5] Simitopoulos D, Koutsonanos D E. Robust image watermarking based on generalized radon transformations. IEEE Transactions on Circuits and Systems for Video Technology, 2003 13(8): 732-745

[6] Xin Y, Liao S, Pawlak M. A multibit geometrically robust image watermark based on zernike moments//Proceedings of the 17th International Conference on Pattern Recognition(ICPR'2004). IEEE Press, 2004: 861-864

[7] Kim H S, Lee H K. Invariant image watermark using zernike moments. IEEE Transactions on Circuits and Systems for Video Technology, 2003, 13(8): 766-775

[8] Chen Q, Yang X L, Zhao J Y. Robust image watermarking with zernike moments[A]//Proceedings of Canadian Conference on Electrical and Computer Engineering (CCECE)[C]. Saskatoon: IEEE Press, 2005: 1340-1343

[9] Farzam M, Shirani S S. A robust multimedia watermarking technique using zernike transforms//IEEE International Workshop Multimedia Signal Processing. 2001: 529-534

[10] Pereira S, Pun T. Robust template matching for affine resistant image watermarking. IEEE Transaction on Image Processing, 2000, 9(6)

[11] Kang Xiangui, Huang Jiwu, et al. A DWT-DFT composite watermarking scheme robust to both affine transform and JPEG compression. IEEE Transactions on Circuits and Systems for Video Technology, 2003, 13(8): 776-786

[12] Lee H-Y, et al. Evaluation of feature extraction techniques for robust watermarking. Berlin Heidelberg: Springer-Verlag, 2005: 418-431

[13] Haddadnia J, Ahmadi M, Faez K. An efficient feature extraction method with pseudo-zernike moment in RBF neural network-based human face recognition system[J]. EURASIP Journal on Applied Signal Processing, 2003(9): 890-901