第 26 卷第 9 期 电子与信息学报 Vol.26No.9
2004 年 9 月 Journal of Electronics & Information Technology Sept. 2004

图像水印抗几何攻击研究综述 [1]

刘九芬 黄达人* 黄继武*

(中国人民解放军信息工程大学信息研究系 郑州 450002)
*(中山大学电子与通信工程系 广州 510275)

摘 要: 稳健性是数字水印技术的一个核心问题. 数字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“稳健性”的声明. 然而, 绝大多数算法所强调的“稳健性”只不过是水印对抗一般信号处理的稳健性, 它们不能抵抗甚至是微小的几何攻击. 本文分析总结了当前图像水印抗几何攻击的各种方法, 提出了下一步可能的发展方向, 对改进和设计水印算法具有一定的指导作用.

关键词: 图像水印, 水印攻击, 几何攻击
中图分类号: TP391 **文献标识码**: A **文章编号**: 1009-5896(2004)09-1495-09

Survey on Watermarking Against Geometric Attack

Liu Jiu-fen Huang Da-ren* Huang Ji-wu*

(*Dept of Information Research, PLA Information Eng. Univ., Zhengzhou* 45002, *China*)

*(*Dept of Electronics and Communication Eng. Zhongshan Univ., Guangzhou* 510275, *China*)

Abstract Robustness is the key issue of digital watermarking technology. Up to now, various watermarking algorithms are proposed with much emphasis on the “robustness”. However, the “robustness” claimed in most of algorithms is only against common signal processing operations such as compression and signal filtering. It is now clear that even very small geometric distortions can prevent the detection of a watermark. In this paper the current methods against geometric attacks are analyzed and summarized, and some probable development directions of digital watermarking at next stage are introduced which are the key issues to improve and design watermarking algorithms.

Key words Digital watermarking, Watermarking attack, Geometric attack

1 引言

数字水印作为一种数据认证和版权保护的手段, 必然会受到各种形式的攻击, 因此稳健性 (Robustness) 是水印系统的一项基本要求, 也是近年来图像水印的主要研究内容. 针对水印处理的不同阶段, 对水印系统的攻击可分为 4 类 [1] : 信号去除攻击 (Removal attacks) 、表示攻击 (Presentation attacks) 、解释攻击 (Interpretation attacks) 和合法攻击 (Legal attacks) . 信号去除攻击涉及到水印信号的去除, 包括“基本攻击” (Basic attack) 、“共谋攻击”和专用的攻击程序等. 表示攻击又称为“同步攻击” (Synchronization attacks) , 它使水印检测失败, 这种攻击不是从有水印的对象中去除水印, 而是将水印变形到检测器检测不出来. 其中最典型的就是几何变形攻击 (Geometrical distortion attack) 和马赛克攻击 (Mosaic attack) . 解释攻击又称“死锁攻击”, 它是通过伪造水印而成功的, 这种攻击造成原来水印不能被判断和不再说明

[1] 2003-10-09 收到, 2004-04-05 改回
国家杰出青年基金 (60325208) 、国家自然科学基金 (30200147 , 60133020) 、河南省高校杰出科研人才创新工程项目 (2003KJCX008) 、中国人民解放军信息工程大学博士启动基金资助课题

任何意义。合法攻击主要是利用法律上一些条款的漏洞以达到攻击的目的，这种攻击大多超出了技术讨论的范围。

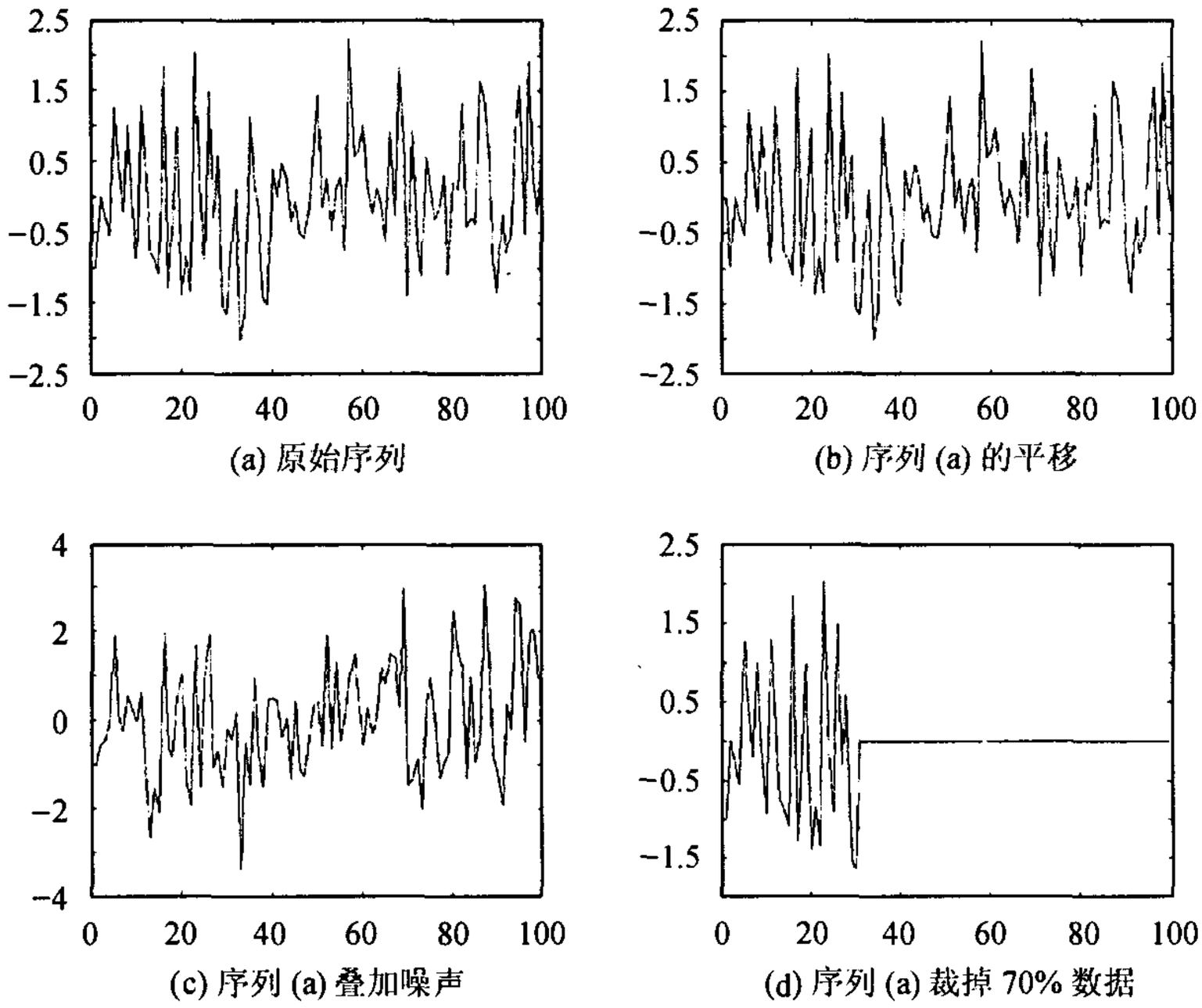
数字水印技术发展到今天，已有大量不同的算法，它们广泛提出了“稳健性”声明。不幸的是，绝大多数水印算法所强调的稳健性只不过是水印对抗一般信号处理 (例如压缩、滤波和噪声干扰等) 的稳健性能。诚然，数字水印技术在应用了嵌入对策、扩频技术、信道编码技术和利用了视觉系统特性提高水印的嵌入强度后，对多数常规攻击的稳健性较好。然而，绝大多数水印算法不能抵抗甚至是微小的几何攻击 [2−5] ，即现有的水印技术抵抗表示攻击的能力很差。因此，抗几何攻击的数字水印技术仍然是一项富有挑战性的工作。

本文主要介绍和分析目前抗几何攻击的主要水印算法，试图说明当前抗几何攻击水印算法所存在的问题和今后可能的发展方向。本文的安排如下：第 2 节简单介绍几何攻击的作用；第 3 节和第 4 节分别介绍非盲检测和盲检测抗几何攻击的水印算法；第 5 节是结论和可能的发展方向。

2 几何攻击的作用

对于给定的水印算法，水印检测器必需知道水印嵌入的确切位置。由于常用的变换 DCT (Discrete Cosine Transform) 、 DWT(Discrete Wavelet Transform) 等不具有几何不变特征，在几何失真后，原有位置系数的值都将产生较大的变化。尽管水印分量从一定意义上讲，仍然可能存在于数字媒体中，但各分量的存在位置已经与嵌入时完全不同。因此，几何攻击破坏了水印分量的同步。如果水印算法中没有设计抵御这种攻击的措施，水印的检测是十分困难的。

一个简单的采用随机序列作为水印的例子如图 1 所示。图 1(a) 为原始水印序列，图 1(b)~图 1 (d) 为改变后的水印序列 (模拟从受攻击后的宿主载体信号中检测的水印) 。图 1(b) 为序列向右平移一个元素，等效为水印的同步受到破坏；图 1(c) 为原始序列叠加一个随机噪声，等效水印数据受到改变。设原始水印序列与其自身的规一化相似性为 1 ，可以计算图 1(b) 、图 1(c) 与图 1(a) 的相似性分别为 0.00 和 0.58 。为了进一步说明水印同步的重要性，我们将图 1(a) 裁掉了 70% 的数据，但不破坏其同步性，得到图 1(d) 。其与图 1(a) 的相似性为 0.61 。这个例子



(a) 原始序列　(b) 序列 (a) 的平移

(c) 序列 (a) 叠加噪声　(d) 序列 (a) 裁掉 70% 数据

图 1　水印序列的同步

说明了在水印检测中，同步问题的重要性。从水印攻击的角度，破坏水印的同步比直接破坏数据更加有效。

目前，水印对抗几何攻击有非盲检测和盲检测的方法。一般来说，盲检测水印算法的稳健性较差。

3 非盲检测抗几何攻击的图像水印

如果水印检测时可以借助于原始图像或者未受攻击的水印图像，则可以从攻击后的水印图像与原始图像的几何关系，估计出水印图像的几何变形，在水印检测前以一定的精确度对水印图像进行相反的几何变换 (如图 2)，从而有效降低水印的检测错误率。从原理上讲，这是一种已知降质的图像恢复方法。对几何变形的水印图像进行恢复，包含二个步骤：

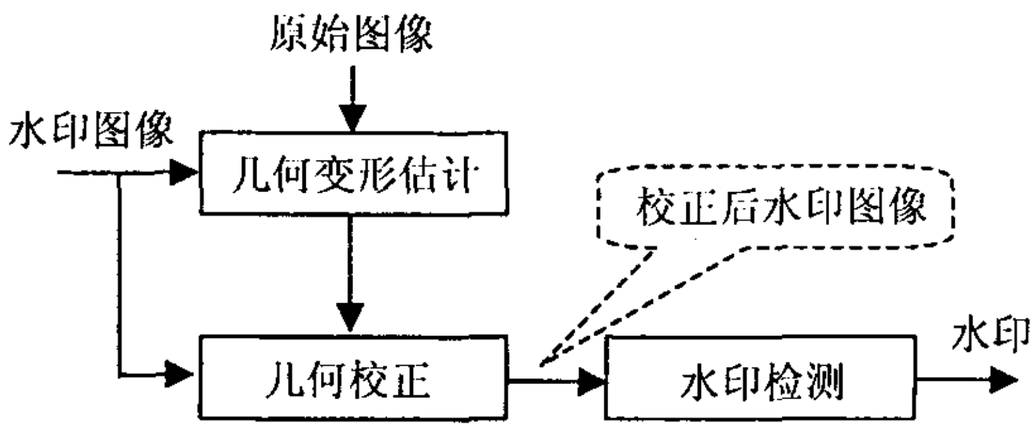


图 2　基于几何校正的水印检测

(1) 借助参考图像，估计水印图像的几何变形类型和相应的参数。

水印所受到的几何攻击包括 RST(Rotation, Scaling, Translation) 、 shearing(剪切) 、线性变换等。

几何变形类型和参数的估计可以采用现有的图像校准 (Image registration) 技术 [6,7] 。从原理上说，图像校准是对不同图像相似性的测量。

图像校准算法可分为基于区域相关法、基于图像几何特征的校准法以及 Fourier 变换法。基于区域相关的校准法，一般在进行处理之前，首先定义区域的大小，并将参考图像划分成若干个分离的临时区域。然后通过改变目标图像上移动区域的位置和大小，来计算它与参考图像上所选区域的相关值，再利用循环比较的计算方法来搜寻一定范围内有最大相关值的位置，其所在位置的坐标和两区域比例因子的大小作为校准公式参数。由于这类方法直接利用图像的像素信息，抗噪声能力差，对旋转攻击处理比较困难，并且计算量大，校准效率低。在基于图像几何特征的校准法中，算法的稳定性主要依赖于特征空间的选取 (点特征、线特征、区域特征等) 、相似性度量、搜索空间、搜索策略等。从实际情况来看，图像几何特征的数量与位置的精确性定位通常很受限制，经常因图像中的几何基本体太简单化而使图像几何特征稀少和不精确。另外，在原始图像中嵌入水印后，图像的特征点往往会偏移 1 至 2 个像素。这容易导致校准精度的下降。基于 Fourier 变换法，利用 Fouirer 变换的性质校准平移和旋转。但对缩放校准困难，旋转校准需进行二维搜索。

由于几何变形事先不可能知道，因此几何变形的类型和参数的估计只能采取搜索判断的策略，这是一项计算量较大的工作。图 3 是估计几何变形类型和参数的流程。对每一种可能的攻击，需要以一定的步长进行逆变换，然后计算逆变换的水印图像与参考图像的相似性，以此决定水印图像的几何变形类型和相应的参数。为了减少计算量，可以采取多分辨率搜索和变化搜索步长的方法。

(2) 根据上述所求出的参数，对水印图像进行几何变换。这种变换是几何变形的逆运算，变换的目的在于抵消几何变形的作用。

由于几何变形的类型和参数的估计本身就是一个先进行逆几何变换，再计算相似性的过程，因此，在完成几何变形类型和参数的估计时，实际上也完成了几何变形的逆变换。

现有的非盲检测抗几何攻击的图像水印算法不多。我们 [8] 在 DWT 域嵌入水印，然后把原始图像当作参考图像，可能已变形的水印图像当成目标图像，依靠现有的图像校准技术，恢复

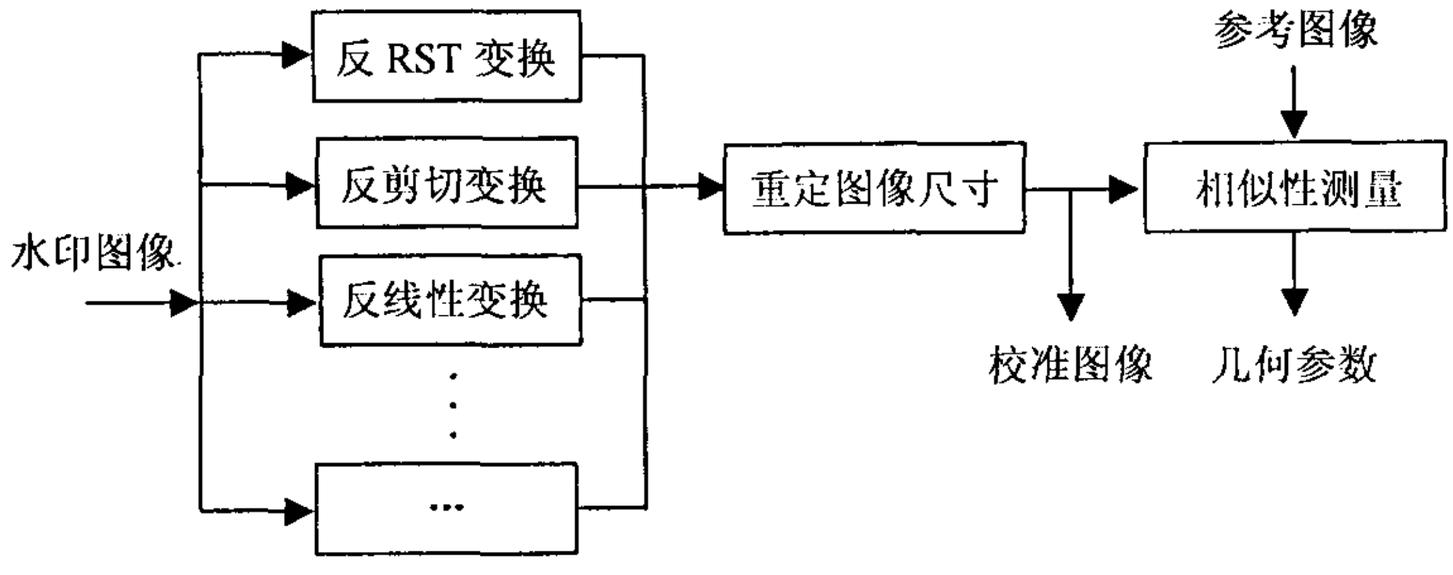


图 3 几何变形类型和参数的估计

几何变形，取得了比较好的效果。其它的非盲检测算法，也是以一定的精确度对所有可能的攻击进行相反的变换，然后确定哪种反变换可提供最好的结果，从而从两幅图像中估计出几何变形，对此变形进行恢复。 Davoine 等 [9] 受到视频编码中运动补偿的启发，将原始图像划分成三角网格，并将该网格作为参照坐标系，在水印检测前对可能已变形的水印图像与参考图像进行运动估值，然后对可能已变形的水印图像进行补偿。但该算法仅对类似帧间运动那么小的变形有效。 Johnson 等 [10] 把不同分辨率和不同角度的图像边缘特征点作为参照坐标系来识别图像的变形和参数，然后恢复几何变形。但由于借助于图像特征点的方法本身精度不够，该算法还需借助于原始图像应用 normal flow 进行精细校正。 Braudaway 等 [11] 在原始图像和水印图像中建立三个以上的参考点，然后采用穷尽搜索的办法找到它们之间的最佳匹配，以此来确定水印图像中每个像素在水平和垂直方向上的变形。我们 [12] 在 DWT 域嵌入水印，并引入距离测量的概念，通过寻找使水印图像和原始图像间的距离最小的反攻击变换，实现水印检测的重同步。

另外，刘瑞祯等 [13] 提出一种基于奇异值分解的单向非对称的水印算法，其特征在于将一幅数字图像设为非负矩阵，进行奇异值分解，将伪随机序列构成的水印嵌入到原始图像的奇异值中。由于奇异值表现的是图像的内蕴特性而不是视觉特性，当图像被施加小的扰动时，图像的奇异值不会有大的变动，从而可以有效抵抗旋转和图像的扫描与打印引起的一些几何变形。

非盲检测的方法由于需要借助于原始图像，或者需要在海量的数据库中寻找未受攻击的水印图像，使得它的应用受到较大的限制。

4 盲检测抗几何攻击的图像水印

在许多应用场合无法确定原始图像，比如图像监控或跟踪，不可能得到原始图像。在其它一些应用，比如视频水印应用，由于要处理的数据量很大，使用原始视频也是行不通的。因此不需要原始数据的盲检测技术具有更广阔的应用领域。

与非盲检测算法相比，具有抗几何攻击的盲检测图像水印的实现更加困难。为了考虑各种可能的水印图像的再定位和大小调整，目前有两种策略可供选择。第一种策略是预防性的，寻找对几何攻击不敏感的特征，把水印嵌入到该特征空间；第二种策略是是治疗性的，通过嵌入一个能够指示出几何攻击参数的辅助信息，以便对被攻击图像的几何变换做后验估计，然后在提取水印前进行相反的变换。

目前抵抗几何攻击的水印方法大致可以分为如下三类。

4.1 利用几何不变量的抗几何攻击图像水印

这类算法的基本思想是从原始图像中找到具有几何不变性的量用来隐藏水印。由于具有几何不变性，在水印图像遭受几何攻击后，这些量没有变化。因而隐藏于其中的水印信息得以保存。该类算法的优点是不用确定并恢复几何攻击，但目前该类算法只能抵抗 RST 。

Fourier-Mellin 变换是一种具有 RST 不变性的变换。 O'Ruanaidh 等 [14] 首先提出把水印嵌入到 Fourier-Mellin 变换域中。该算法第一步计算图像 DFT(Discrete Fourier Transform) 。因为图像在空间域内的线性平移只是引起 Fourier 变换域内的相位线性平移，而幅值不变，因此如果水印嵌入到幅值的子空间里，它对于空间坐标平移具有不变性。第二步，对 DFT 的幅值进行 LPM(Log-Polar Map) ，这时笛卡儿坐标系变为对数极坐标系。笛卡儿坐标系中的缩放和旋

转对应于对数坐标系中的平移。第三步再对对数极坐标上的系数做 DFT，只取 DFT 的幅值，那么得到的空间具有 RST 不变性。水印嵌入到该空间可以对抗 RST。水印图像由两次逆 DFT 和一次逆 LPM 得到。事实上，该算法仅仅是理论上的，文献 [14] 中提到的困难限制了它的应用；而且在 512×512×8 bit 图像上嵌入的信息量也只有 13 个字符。值得说明的是，该算法实际上是第一个专门设计抵抗几何攻击的算法。它的一个简单变形是 Wu 等 [15] 基于 Radon 变换的算法。Lin 等 [16] 改进了 O'Ruanaidh 的方法，不是作两次 DFT 得到“强不变量”而是只作一次 DFT。该算法把图像 DFT 的幅度谱重采样后做 LPM，再沿着坐标轴 $\log(r)$ 把幅度系数连加得到一维函数，最后把水印加载到该函数上。那么水印平移不变；对水印图像的旋转攻击，只是引起水印的一个平移，利用简单的搜索来补偿；对水印图像的缩放攻击，只是引起水印能量减弱或加强，利用相关检测度量来补偿。但检测的结果只是 0 或 1(即水印的存在与否)，即信息量只有 1 bit。上述算法有两个主要缺点：(1) 使用这种策略的水印只能抵抗 RST，不能同时抵抗剪切、长宽比 (Aspect ratio) 改变和 RST 联合攻击中常伴随的剪切等其它攻击；(2) 当坐标系变化时，即进行 LPM 和逆 LPM 时，由于需要某种形式的插值会导致水印图像质量急剧下降。Lin[17] 提出的方法是一个与文献 [14] 类似的方法，用 Log-Log Map (LLM) 代替 LPM，由于笛卡儿坐标系中 x 和 y 轴不同比例的缩放对应于对数－对数坐标系中的平移，因此可以抵抗图像长宽比的改变，但不能抵抗旋转，它同样需要某种形式的插值，而且在 512×768×8 bit 图像上嵌入信息也只有 56 bit。

利用 DFT 的性质，直接在 DFT 域的某些特定系数上嵌入水印，也是一种可能的考虑。比如，可以把水印隐藏在 DFT 幅度谱的零频率为中心的圆周或圆环上，都可以生成满足一定几何不变性的水印。Pitas 等 [18] 提出了把二值水印嵌入以图像 DFT 幅度谱的零频率为中心的圆环中。这种方法能抵抗平移、缩放和旋转角度不大于 3° 的旋转，嵌入的信息量也只有 1 bit。Lick 等 [19] 在文献 [18] 的基础上，提出在 DFT 幅度谱的中频带的某一圆周上嵌入伪随机序列，只是克服了 Pitas 方法在抵抗旋转方面的局限性，但对长宽比的改变或裁剪一行或一列将会导致水印检测失败，检测的结果也只是 0 或 1。后两种方法与前两种方法不同，不是把水印嵌入到 RST 的不变域中而是不管 RS 攻击的影响，因此后两种方法不用 LPM，从而避免了应用 LPM 引起的水印图像质量的急剧下降。

对水印攻击最常见的例子是打印和扫描过程引起的形变。文献 [17,20] 给出了打印和扫描的模型。文献 [20] 还给出了几种提取几何不变量的方法。

需要注意的是，目前该类算法只利用了 DFT 的幅度成分，未用相位成分。而 Hays 等 [21] 研究表明，对图像理解而言，相位比幅度更重要。因此如何同时利用幅度和相位成分是该类算法的一个发展方向。

4.2 利用辅助信息的抗几何攻击图像水印

我们清楚，只要知道图像水印的几何变化，通过实施逆变换，就有可能重同步并检测出水印。因此，在隐藏水印的同时，嵌入一个能指示出图像几何变化的辅助信息是一种很直接的思路。必须注意到，辅助信息的数据量应该尽可能小。

有一类抵抗几何攻击的算法是将一个可识别的结构嵌入到空间中。水印检测之前，由提取的结构信息纠正水印图像可能遭受的几何攻击。Fleet 等 [22] 将正弦曲线嵌入到图像的颜色通道中。该正弦曲线信号作为一个参考坐标系能用来校正水印图像。Gruhl 等 [23] 提出通过改换图像平面的最不重要位 (Least Significant Bit LSB) 将不可见交叉号嵌入到图像中。之后，对交叉号的检测可以确定水印所经过的攻击，并由此来进行畸变修正。如果还要确保对裁剪的抵御，则除了交叉号外，行和列的信息也被编码。但这个系统的稳健性不高，因为水印参考信息很容易被去除或破坏。Kutter[24] 提出一种对文献 [23] 的扩展方法，提出在图像的 4 个平移位置各嵌入一个参考水印模式，水印的自相关函数可以反映图像所遭受的几何攻击。四个由随机序列组成的水印信息有关，它们是彼此的移位序列。初始序列模式是一个二维伪随机序列，根据预先确定的水平偏移 δ_x 和垂直偏移 δ_y，第二个模式是初始序列在水平方向上平移 δ_x 列，第三个模式是初始序列在垂直方向上平移 δ_y 列，第四个模式是初始序列在水平方向上平移 δ_x 列、垂直方向上平移 δ_y 列。四个模式交织嵌入：初始序列奇行奇列嵌入，第二个模式奇行偶列

嵌入，第三个模式偶行奇列嵌入，第四个模式偶行偶列嵌入。这样，同一随机数嵌在四个不同的位置： (x,y) ， $(x+2\delta_x+1,y)$ ， $(x,y+2\delta_y+1)$ ， $(x+2\delta_x+1,y+2\delta_y+1)$ 。在水印提取过程中，通过应用一个预滤波器，计算出一个可以估计出水印模式的二维自相关函数。自相关函数有 9 个极值点，中心的极值点代表滤波后图像的能量，强度最大，而其它对称于中心点的 8 个点是由 4 个嵌入的随机序列的自相关函数产生。这些极值点的结构与从可能遭受几何攻击的水印图像抽取的极值点的结构相比，决定水印图像所遭受的仿射变换。实验结果表明：该算法可以抵抗一般的几何变换包括长宽比改变、旋转和剪切等。它的主要缺点： (1) 易受压缩的影响； (2) 由于水印嵌入在空间域内，自相关函数不能检测平移，从而不能抵抗裁剪。在 512 ×512×24 bit 图像上嵌入的信息量是 34 bit ，其中 2 bit 扩频后用于恢复水印所遭受的几何变形。类似算法还有不少 [25−27] 。

另一类抵抗几何攻击的算法是在变换域嵌入一个模板 (Template) 作为校准因子。由于 DFT 在几何变换方面具有较好的性质，目前该类算法的模板都嵌入到 DFT 系数中，不同的算法体现在组成模板的点数、强度和嵌入位置的不同。模板由 Fourier 幅度谱中人为生成的极值点组成，也就是改变一些 Fourier 系数的幅度成为极值点。模板的强度由 Fourier 幅度谱的局部统计值自适应决定。水印检测时，利用小的检测窗检测 Fourier 幅度谱的所有极大值点，通过模板点和检测到的极值点的匹配，确定水印图像遭受的几何变换。除文献 [28,29] 外，该类算法的水印也嵌入到 DFT 系数中，平移不变。 Pereira 等 [28] 把 4 个字符构成的有意义水印自适应嵌入到 512×512×8 bit 图像的 LOT(Lapped Orthogonal Transform) 域的高频成分。该算法在 DFT 系数嵌入模板，可以抵抗缩放因子不小于 0.65 的缩放、旋转和一定大小的裁剪。 O'Ruanaidh 等 [30] 利用平移不变量构造裁剪不变量，用 LPM 补偿旋转和缩放，用 LLM 补偿图像长宽比改变，因而可抵抗裁剪、 RST 或图像长宽比改变，在 512×512×8 bit 图像上嵌入的信息量是 13 个字符。 Pereira 等 [31] 和文献 [30] 非常相似，只不过在 512×512×8 bit 图像上嵌入的信息量是 10 个字符。以上两个算法利用 LPM 只能检测旋转和缩放因子，利用 LLM 只能检测长宽比的改变，一般变换不能恢复。 Pereira 等 [32] 提出一个可以恢复一般仿射变换的算法。同时在模板匹配时，因为抽取的极值点可能不是模板点，该算法提出了一个方法修剪搜索空间降低算法的计算复杂度。模板匹配过程中可能需要一些迭代才能得到一个精确的仿射矩阵，此矩阵决定水印图像可能遭受的几何攻击。一旦仿射变换确定，对水印图像进行逆仿射变换，就可在 Fourier 变换域内检测到水印。该算法隐藏的信息量大约为 60 bit 。在此基础上，我们 [29] 在 DWT 域嵌入 45 个字符构成的水印，用直接序列扩频嵌入到 DWT 低频带作平移同步，在水印图像的 DFT 域嵌入 28 个模板点，平均在两条直线上。由于一条模板线上的模板点在经历了线性变换后仍是局部极大点且在同一条过原点的直线上，因此极大地降低了算法的计算复杂度。 Csurka 等 [33] 应用文献 [31] 的方法抵抗旋转、缩放或裁剪， Deguillaume 等 [34] 把文献 [31] 的算法推广到三维 (视频) 信号。该类算法还有文献 [35,36] 。

需要指出，利用嵌入辅助信息来抵抗几何攻击的方法存在几个弱点： (1) 如果辅助信息的检测失效，将导致水印检测的失败。 (2) 利用这种方法的水印图像都有一个共同的辅助信息，因此易遭受共谋攻击。目前基于模板的水印算法已被文献 [37,38] 简单地利用局部插值而攻击掉。 (3) 辅助信息将或者降低水印图像的质量或者减少水印的数据量。因此，设计安全、稳健、“好”的模板是一个十分重要的课题，是该类算法下一步要解决的问题。

4.3 第二代水印

现有的水印算法大都应用像素或者变换系数嵌入信息，这样的技术被称为第一代水印方案。这种方法的缺点是水印不是嵌入数据视觉的最重要部分。 Kutter 等 [39] 提出了第二代数字水印的概念，它考虑的不是应用像素或者变换系数，而是应用数据的重要特征来嵌入水印信息。所谓的第二代水印由于把水印与图像连结在一起，在稳健性方面有很大的提升能力，因此很具生命力。当然系统的稳健性依赖于特征的选择方法和水印的嵌入技术。

并不是所有的特征都适合于水印， Kutter 等提出了适合于水印的视觉重要特征一般具有的性质： (1) 对噪声不敏感 (有损压缩，加性、乘性噪声等) 。这意味着只有重要的特征适合于水印，因为攻击不会改变这些重要特征，否则图像的商业价值将丢失。 (2) 协变于几何变换 (旋

转、平移、下采样、长宽比改变等)。描述了图像受到几何攻击时特征应有的变化，并且适度的几何调整不应破坏或改变特征。(3) 局部性 (图像裁剪不会改变剩下的特征点)。意味着特征应该有较好的局部属性，使得水印算法能抵抗图像裁剪等。寻找提取适合于水印的特征的提取算法是一个很具挑战性的工作， Celik 等 [40] 提出了几个解决这一问题的方案，并分析了这些方案在理论和实践上的限制。

具备上述性质的特征可以以两种方式应用： (1) 用于水印检测的参考点； (2) 直接用于嵌入水印。 Celik 等 [40] 分析了把特征用于水印检测参考点的水印算法。他们把这类算法分成三部分： (1) 特征点的提取； (2) 基于特征点的图像剖分和剖分后区域的校准； (3) 水印的嵌入和抽取。 Celik 等讨论了算法每一部分的需要和满足要求的解决方案以及方案在理论和实践上的限制。基于文献 [40] 最直接的例子是 Bas 等 [41] 提出的算法。 Kutter 等 [39] 也提出了一个这方面的例子，但缺少了文献 [40] 的剖分后区域的校准，从而该算法不能恢复仿射变换等带来的几何形变。该算法首先对图像进行 Mexican-hat 小波分解，然后按照特征点最邻近区域将图像划分为若干部分。在各部分中分别嵌入扩频水印。由于寻找的特征点具有平移、裁剪协变性，从而可以抵抗这些几何变形。抵抗旋转、缩放变形通过应用 LPM 变换寻找旋转角度和缩放因子来完成。此方法局部化了水印的嵌入和提取过程。 Kaewkammerd 等人 [42] 提出了一个基于 DWT 和特征的水印算法。该算法把一个无意义的伪随机序列组成的水印嵌入到小波分解最高级别的高频带的大系数 (图像的边界和纹理) 中，即把水印直接嵌入到特征点，但它还把一部分特征点作为水印检测的参考点。

如何提取合适的特征、应用这些特征是该类算法需要进一步研究的问题。

5 结论和可能的发展方向

本文分析综合了目前抗几何攻击的水印算法，可以看出水印对抗几何攻击是一个十分困难而极具挑战性的课题。通过采用 Fourier-Mellin 变换构造几何不变特征、隐藏几何校正模型、将水印以一个可识别的结构嵌入到载体数据中和基于原始数据的重要特征等，为水印抵抗几何攻击问题提供了一些可能的解决方向。但还存在许多问题： (1) 抗大面积剪切、 Random bend 等的稳健性尚未得到解决。 (2) 抗一些几何攻击的有意义水印算法嵌入的数据量少。 (3) 基本上讨论的是对图像的整体几何攻击，而未讨论对图像的局部几何攻击。 (4) 目前大多数抗几何攻击水印算法基于经典 Fourier 变换，但 Fourier 变换与 DWT 、 DCT 相比，存在自身的弱点，难以成为主流算法。

为了战胜几何攻击，未来的水印软件应设计成为能容忍通常的几何攻击，并与人进行交互才能进行成功的检测。根据水印抗几何攻击的研究现状分析，一些研究思路和可能的发展方向如下：

(1) 综合利用第二代水印的优点和现有技术无疑很具生命力。基于 DWT 域的水印算法要注意应用 DWT 的多分辨率特性、时频局部化特性和局部的时频的对应性。

(2) 利用几何变形在局部几乎都是线性的这个事实 (等价于平移和旋转)，用基于块的检测算法，对抗局部几何攻击。

(3) 应用信道编码技术、位置随机置乱和交织技术来提高抗裁剪的稳健性。

(4) 应用密码学、数字认证和数字签名或者数字信封等技术，以对抗各种攻击。

参　考　文　献

[1] Crave S, Yeo B L, Yeung M. Technical trials and legal tribulations. *Communications of the ACM*, 1998, 41(7): 45–54.

[2] Petitcolas F A P, Anderson R J, Kuhn M G. Attacks on copyright marking system. In Proc. 2nd Int. Workshop Information Hiding, Portland, OR, Apr. 14-17, 1998: 218–238.

[3] Unzign. http://www.altern.org/watermark.

[4] Cox I J, Linnartz J. Public watermarks and resistance tampering. In Proc of ICIP'97, Washington, DC, 1997: 26–29.

[5] Cox I J, Linnartz J. Some general methods for tampering with watermarks. *IEEE J. on Selected Areas in Communications*, 1998, 16(4): 587–593.

[6] Brown L G. A survey of image registration techniques. *ACM Computing Surveys*, 1992, 24(4): 325–376.

[7] Thévenaz P, Ruttimann U E, Unser M. A pyramid approach to subpixel registration based on intensity. *IEEE Trans. on Image Processing*, 1998, 7(1): 27–41.

[8] 刘九芬, 王振武, 黄达人. 抗几何攻击的小波变换域图像水印算法. 浙江大学学报 (工学版), 2003, 37(4): 386–392.

[9] Davoine F. Watermarking et résistance aux deformation géométriques. In Cinquiemes journées d'études et d'échanges sur la compression et la representation des signaux audiovisuals (CORESA'99), Centre de Recherché et Développement de France Télécom (Cnet), EURECOM, Conseil Général des Alpes-Maritimes and Télécom Valley, Sophia-Antipolis, France, Jun. 1999: 14–15.

[10] Johnson N F, Duric Z, Jajodia S. Recovery of watermarks form distorted images. In Proc. 3^{rd} Int. Information Hiding Workshop, Dresden, Germany, 1999: 361–375.

[11] Braudaway G W, Minter F. Automatic recovery of invisible image watermarks from geometrically distorted images. In Proc. SPIE Security and Watermarking of Multimedia Contents I, CA, USA, 2000, Vol.3971: 74–81.

[12] Kang X G, Huang J W, Shi Y Q. An image watermarking algorithm robust to geometric distortion. Lecture Notes in Computers Science: Proc. of IWDW 2002, Spinger-Verlag, 2002, Vol. 2613: 212–213.

[13] 刘瑞祯, 谭铁牛. 基于奇异值分解的数字图像水印方法. 电子学报, 2001, 29(2): 168–171.

[14] O'Ruanaidh J J K, Pun T. Rotation, scale and translation invariant spread spectrum digital image watermarking. *Signal Processing*, 1998, 66(3): 303–317.

[15] Wu M, Miller L M, Bloom J A, *et al.*. A Rotation, scale, and translation resilient public watermark. In Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing 1999(ICASSP'99), Phoenix, AZ, 1999. http://www.assuredigit.com/tech_doc/more/Cox_Rotation_ scaling_translation_resilient_public_watermark. PDF

[16] Lin C Y, Wu M, Bloom J A, *et al.*. Rotation, scale, and translation resilient watermarking for images. *IEEE Trans. on Image Processing*, 2001, 10(5): 765–782.

[17] Lin C Y. Public watermarking surviving general scaling and cropping: An application for print-and-scan process. Multimedia and Security Workshop at ACM Multimedia 99, Orlando, FL, USA, Oct. 1999. http://citeseer.ist.psu.edu/lin99public.html

[18] Solachidis V, Pitas I. Circularly symmetric watermark embedding in 2-D DFT domain. IEEE Int. Conf. on Acoustics, Speech and Signal Processing (ICASSP'99), Phoenix, 1999, Vol. 6: 3469–3472.

[19] Licks V, Jordan R. On digital image watermarking robust to geometric transformations. IEEE Int. Conference on Image Processing, Vancounver, Canada, 2000: 690–693.

[20] Lin C Y, Chang S F. Distortion modeling and invariant extraction for digital image print-and-scan process. International Symposium on Multimedia Information Processing (ISMIP 99), Taipei, Taiwan, Dec. 1999. http://www.ctr.columbia.edu/papers_advent/99/cylin-modelscan.pdf

[21] Hayes M H. The reconstruction of a multidimensional sequence from the phase or magnitude of the FFT. *IEEE Trans. on Acoustics, Speech and Signal Processing*, 1992, (4): 140–154.

[22] Fleet D J, Heger D J. Embedding invisible information in color images. In Proc. IEEE Int. Conf. on Image Processing (ICIP-97), Santa Barbara, October 1997, 1: 532–535.

[23] Gruhl D, Bender W. Affine invariance. http://nif.www.media.mit.edu/DataHiding/affine/affine.html, 1995.

[24] Kutter M. Watermarking resistance to translation, rotation, and scaling. In Proc. SPIE Multimedia Systems Applications, 1998, Vol. 3528: 423–431.

[25] Honsinger C, Rabbani M. Data embedding using phase dispersion. In PICS 2000: Image Quality, Image Capture, Systems Conf., 2000, 3: 264–268.

[26] Honsinger C W, Daly S J. Method for detecting rotation and magnification in image. U. S. Patent, 5835639, 1998.

[27] Voloshynovskiy S, Deguillaume F, Pun T. Content adaptive watermarking based on a stochastic multiresolution image modeling. In EUSIPCO 2000, Tampere, Finland, September, 2000. http://citeseer.ist.psu.edu/380994.html

[28] Pereira S, O'Ruanaidh J J K, Pun T. Secure robust digital watermarking using the lapped orthogonal transform. In IST/SPIE Electronic Image'99, Session: Security and Watermarking of Multimedia Contents, San Jose, CA, USA, January 1999. http://citeseer.ist.psu.edu/pereira99-secure.html

[29] Kang X G, Huang J W, Shi Y Q, *et al.*. A DWT-DFT composite watermarking scheme robust to both affine and JPEG compression. *IEEE Trans. on Circuits and Systems for Video Technology*, 2003, 13(8): 776–786.

[30] O'Ruanaidh J J K, Pereira S. A secure robust digital image watermark. In Electronic Imaging: Processing, Printing and Publishing in Colour, SPIE Proceedings, Zürich, Switzerland, May 1998. (SPIE/IST/Europto Symposium on Advanced Imaging and Network Technologies). http://citeseer.ist.psu.edu/181609.html

[31] Pereira S, O'Ruanaidh J J K, Deguillaume F, *et al.*. Template based recovery of Fourier-based watermarks using log-polar and log-log maps. IEEE Int. Conf on Multimedia Computing and Systems (ICMCS'99), Florence, Italy, June 1999. http://citeseer.ist.psu.edu/pereira99template.html

[32] Pereira S, Pun T. Fast robust template matching for affine resistant image watermarks. In Proc. 3^{rd} Int. Information Hiding Workshop, Dresden, Germany, 1999: 207–218.

[33] Csurka G, Deguillaume F, O'Ruanaidh J J K, *et al.*. A Bayesian approach to affine transformation resistant image and video watermarking. In Proc. 3rd Int. Information Hiding Workshop, Dresden, Germany, 1999: 315–330.

[34] Deguillaume F, Csurka G, O'Ruanaidh J J K, *et al.*. Robust 3D DFT video watermarking. In IST/SPIE Electronic Imaging'99, Session: Security and Watermarking of Multimedia Contents, San Jose, CA, USA, January 1999, Vol.3657: 113–124.

[35] Digimarc Corporation, Photographic Products and Methods Employing Embedded Information, US patent 5822436, 1999.

[36] Piva A. Improving DFT watermarking robustness through optimum detection and synchronization, Multimedia and Security Workshop at ACM Multimedia'99, GMD, Department of Electronic Engineering, University of Florence, Italy: Report 85.

[37] Voloshynovskiy S, Pereira S, Iquise V, *et al.*. Attack modeling: Towards a second generation watermarking benchmark. *Signal processing*, 2001, 81(6): 1177–1214.

[38] Herrigel A, Voloshynovskiy S, Rytsar Y. The watermark template attack. In Security and Watermarking of Multimedia Contents III, Wong P W, Delp E J, Eds. SPIE Photonics West, Electronic Imaging 2001, San Jose, CA, USA, Jan. 2001, Vol.4314: 394–405.

[39] Kutter M, Bhattacharjee S K, Ebrhimi T. Towards second generation watermarking schemes. ICIP'99, Kobe, Japan, October 25-28, 1999, Vol. 3: 320–323.

[40] Celik M U, Saber E, Sharma G, *et al.*. Analysis of feature-based geometry invariant watermarking. In Proceedings of SPIE: Security and Watermarking of Multimedia Contents III, Jan. 2001, Vol. 4314: 261–268.

[41] Bas P, Chassery J M, Macq B. Robust watermarking based on the warping of pre-defined triangular patterns. In Proceedings of SPIE: Security and Watermarking of Multimedia Contents II, San Jose, CA, USA, Jan. 2000, Vol. 3971: 99–109.

[42] Kaewkamnerd N, Rao K R. Wavelet based watermarking detection using multiresolution image registration. TENCON 2000, Kaula Lumpur, Malaysia, Sept. 2000. http://www-ee.uta.edu/dip/paper/tencon_water.pdf

刘九芬：　女，1963 年生，副教授，研究方向：小波理论及其应用、信息隐藏与数字水印.

黄达人：　男，1945 年生，教授，研究方向：小波理论及其应用、信息隐藏与数字水印.

黄继武：　男，1962 年生，教授，研究方向：信息隐藏与数字水印、图像处理.