

结合 Zernike 矩和模板具有 RST 不变性的 DWT-HMM 鲁棒水印算法

王春桃¹⁾ 倪江群^{1),2)} 黄继武^{1),2)} 张荣跃¹⁾

¹⁾(中山大学电子与通信工程系,广州 510275) ²⁾(广东省信息安全技术重点实验室,中山大学,广州 510275)

摘要 抵抗几何攻击是鲁棒水印研究的关键问题之一。为实现水印同步,提出了一种结合 Zernike 矩和小波域模板实现由粗到精几何同步的算法,即首先利用平移归一化图像的 Zernike 矩估计旋转和缩放参数,并用校正旋转和缩放后的图像和原图像之间的质心增量估计平移参数;然后基于粗略估计的参数,通过匹配小波域模板实现旋转、缩放和平移(RST)参数的精确识别和校正,该同步方法可以较大程度地降低搜索空间。水印嵌入和检测采用了小波域向量隐马尔可夫模型(DWT-HMM)。仿真结果表明,利用由粗到精的几何同步方法和基于 HMM 的水印算法能有效抵抗 StirMark 平台的多种单项攻击和联合攻击,算法具有较好的鲁棒性能。

关键词 数字水印 Zernike 矩 几何变形 鲁棒性 小波域隐马尔可夫模型 模板

中图法分类号: TP911.73 **文献标识码**: A **文章编号**: 1006-8961(2008)07-1250-08

A RST-invariant Robust DWT-HMM Watermarking Algorithm Incorporating Zernike Moment and Template

WANG Chun-tao¹⁾, NI Jiang-qun^{1),2)}, HUANG Ji-wu^{1),2)}, ZHANG Rong-yue¹⁾

¹⁾(Department of Electronics and Communication Engineering, Sun Yat-Sen University, Guangzhou 510275)

²⁾(Guangdong Key Laboratory of Information Security Technology, Sun Yat-Sen University, Guangzhou 510275)

Abstract One of the key issues for robust watermarking is to resist geometrical attacks. A matching strategy from coarse to fine scale to achieve the geometrical synchronization incorporating Zernike moments and the template in wavelet domain is proposed. At the coarse stage, the rotation and scaling parameters are estimated with the Zernike moments of the translation-normalized image, while the translation parameters are estimated with the centroid's increments between the original image and the image that are corrected for rotation and scaling. At the fine stage, the accurate values of rotation, scaling, and translation (RST) are obtained by matching the template around the roughly estimated RST values, which hence reduces the searching spaces to some extent. Finally, the attacked image is corrected with the accurate RST values. A watermarking scheme based on the vector Hidden Markov Model in wavelet domain (DWT-HMM) is also adopted. Good robustness is observed against StirMark attacks and their joint attacks.

Keywords digital Watermarking, Zernike Moments, geometric Distortion, robustness, DWT-HMM, template

1 引言

近年来,作为数字多媒体版权保护的新方法,数

字水印技术受到了业界的广泛关注,并得到了深入的研究^[1,2]。如何提高水印抵抗几何攻击的性能是鲁棒水印研究中的关键问题。对水印的几何攻击既包括全局性的旋转、平移、缩放、裁剪(cropping)和剪切

基金项目:国家自然科学基金项目(60773200);广东省自然科学基金项目(7003722)

收稿日期:2006-03-28;**改回日期**:2007-03-21

第一作者简介:王春桃(1979~),男。2007年于中山大学获无线电物理专业博士学位。主要研究方向为多媒体信息安全。E-mail:

wct2006@gmail.com

(shearing)等几何变换,也包括局部性的随机弯曲、局部几何变换等^[3]。由于几何攻击引起的几何失真会引起水印失步问题,从而导致水印检测失败^[4]。

对于抵抗几何攻击的方法,根据是否利用原图像可以分为“非盲”和“盲”两类方案,前者需要原图像辅助,而后者则无需原图像^[3,5]。但现实应用中接收端通常无法获得原图像,因此目前的研究主要以“盲”方案为主。当前已有的各种抵抗几何攻击的“盲”方案可以分为以下4类:(1)将图像变换到几何变换不变域,然后在不变域中嵌入水印信息,如 Fourier-Mellin 变换^[6]、基于 Zernike 矩的水印算法^[7,8]和对图像进行归一化的水印算法^[9,10];(2)周期性重复插入多个水印序列,通过互相关函数进行检测^[3,5];(3)利用与图像内容有关的特征点来嵌入水印信息^[3,9];(4)在图像的空域或其他变换域(如 DFT 域)中嵌入模板^[3,5]。

通过模板来抵抗几何攻击,能较好地实现全局性和局部性的几何同步,但通常搜索计算量很大^[11]。本文提出了一种由粗到精的模板匹配算法,可以较大幅度地降低搜索空间,提高模板匹配效率。首先利用平移归一化图像的 Zernike 矩^[10,12]估计出缩放和旋转角度参数,并用校正或近似校正旋转和缩放后的图像和原图像间的质心增量来估计平移参数;然后基于这些估计参数在一个相对较小的范围内匹配小波域模板来获取准确的 RST(旋转、缩放和平移)值,并用它们来校正受攻击的图像。需要指出的是,与文献[7]和文献[8]中基于 Zernike 矩的鲁棒水印算法不同,本文是利用 Zernike 矩来估计旋转和缩放参数而不是像文献[7,8]那样直接在 Zernike 矩上嵌入水印信息。

在先前的工作中,曾提出了基于小波域向量隐马尔可夫模型(DWT-HMM)的图像水印算法^[13]。向量 DWT-HMM 可以准确刻画图像小波域不同尺度和同一尺度不同方向子带小波系数间的真实分布及能量相关性^[14,15];基于向量 DWT-HMM,并综合应用扩频技术、视觉自适应掩盖、信道编码和针对向量 HMM 树形结构的最优水印嵌入策略,实现了水印的鲁棒嵌入和检测^[13]。

通过采用 Zernike 矩和小波域模板由粗到精地识别和抵抗几何攻击,以及运用向量 DWT-HMM 来嵌入和检测水印,本文水印算法可以有效抵抗基于 StirMark 4.0^[16]平台的各种单项攻击(如 RST、剪切、JPEG 压缩、锐化)以及基于这些攻击的联合攻击,表现出了良好的鲁棒性。

2 模板和水印的嵌入与检测

鲁棒水印算法包括多比特水印的嵌入和检测以及模板的嵌入和检测两部分。水印信息的嵌入和检测采用文献[13]中提出的基于小波域向量 HMM 模型的水印算法。该算法基于向量 DWT-HMM 在 $HH_i, HL_i, LH_i (i=3,4)$ 子带中实现了多比特水印信息的鲁棒嵌入和检测。

本文算法同时采用 Zernike 矩和模板实现受几何攻击水印图像的同步,其中 Zernike 矩用于粗略估计 RST 参数值,而模板用于精确估计 RST 参数值。算法中的模板由随机序列构造,考虑到经扩频后的水印信息嵌入在 $HH_i, HL_i, LH_i (i=3,4)$ 子带中^[13],为尽可能避免模板短随机序列对嵌入水印信号的影响,算法中将模板嵌入在 LL 子带中。水印算法的基本流程如图1所示,对原图像作4层小波分解,据文献[13]的算法将经扩频和信道编码的水印信号嵌入在 $HH_i, HL_i, LH_i (i=3,4)$ 子带中,然后在小波反变换到第2层时再将模板嵌入到 LL_2 中,该处理流程可以同时兼顾水印信号和模板的鲁棒嵌入。

首先用密钥 k_1 作为种子产生一个随机序列向量 $S\{s_i; s_i \in \{-1, +1\}, i=1, 2, \dots, 64\}$,并构造 8×8 形式,作为嵌入用的模板;然后基于密钥 k_2 在 LL_2 中选取一个 8×8 的区域用于模板嵌入。为了抵抗裁剪,通常将此区域选择为靠近 LL_2 几何中心的区域。嵌入方法^[5]为

$$S'(i) = S(i) - (S(i) \bmod \alpha) + \frac{3}{4}\alpha$$

$$x_i = 1 \text{ 且 } (S(i) \bmod \alpha) \geq \frac{1}{4}\alpha$$

$$S'(i) = \left[S(i) - \frac{1}{4}\alpha \right] - \left[\left(S(i) - \frac{1}{4}\alpha \right) \bmod \alpha \right] + \frac{3}{4}\alpha$$

$$x_i = 1 \text{ 且 } (S(i) \bmod \alpha) < \frac{1}{4}\alpha$$

$$S'(i) = S(i) - (S(i) \bmod \alpha) + \frac{1}{4}\alpha$$

$$x_i = 0 \text{ 且 } (S(i) \bmod \alpha) \leq \frac{3}{4}\alpha$$

$$S'(i) = \left(S(i) + \frac{1}{2}\alpha \right) - \left[\left(S(i) + \frac{1}{2}\alpha \right) \bmod \alpha \right] + \frac{1}{4}\alpha$$

$$x_i = 0 \text{ 且 } (S(i) \bmod \alpha) > \frac{3}{4}\alpha. \quad (1)$$

其中, α 为嵌入强度控制因子,其值由实验确定。

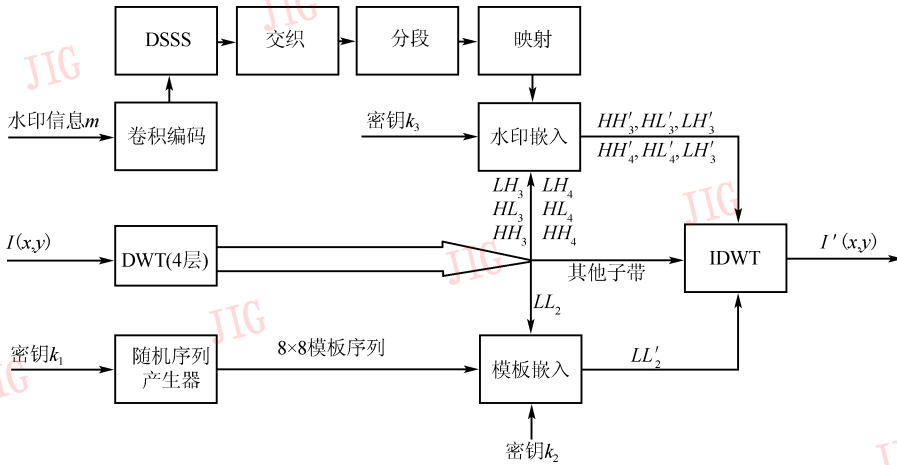


图 1 模板和水印的嵌入

Fig. 1 Embedding of the template and watermark

假设 $G'(x,y)$ 为已经用第 3 节的几何同步方法校正几何攻击后的图像, 将 $G'(x,y)$ 进行 4 层小波金字塔分解, 然后利用 LL_2 来检测模板。与模板嵌入时类似, 用密钥 k_2 选取一个 8×8 的区域作为模板序列的检测区域。设 $S'(i)$ ($i = 1, 2, \dots, 64$) 为该检测区域中一个值, 则检测方法为

$$t_i = \begin{cases} +1 & (S'(i) \bmod \alpha) > \frac{\alpha}{2} \\ -1 & \text{其他} \end{cases} \quad (2)$$

检测完该区域后可以获得一个检测序列 $T = \{T_i; T_i \in \{-1, +1\}, i = 1, 2, \dots, 64\}$ 。

为了考察此模板序列的可信程度, 需要计算检测模板序列 T 和原模板序列 S 的相关值。由于序列都是 $\{-1, +1\}$ 的集合, 故 T 和 S 的相关值为

$$\rho_{T,S} = \frac{1}{64} \sum_{n=1}^{64} (T_n \times S_n) \quad (3)$$

当 $\rho_{T,S}$ 大于或等于某个阈值 T_p 时, 认为成功地检测到模板。

设阈值为 T_p , 则最大误比特数个数为 $e = \lceil 32(1 -$

$T_p) \rceil$ 。据 e 可求得虚警概率为 $H_{fp} = \left(\frac{1}{2}\right)^{64} \sum_{k=1}^e C_{64}^k$, 在实际中则可由给定的虚警 H_{fp} 确定阈值 T_p 。

3 基于 Zernike 矩的几何同步

设接收端接收到的图像为 $G(x,y)$, 则它可能是嵌入模板和水印后的图像 $I'(x,y)$ 在遭受包括几何攻击在内的各种攻击后的版本。为了能无误地从 $G(x,y)$ 中提取水印信息, 必须识别 $G(x,y)$ 所受的几何攻击并进行校正, 这一同步过程采用结合 Zernike 矩和小波域模板的由粗到精的策略来实现。首先用平移归一化后图像的 Zernike 矩估计旋转和缩放参数, 并用校正旋转和缩放参数后的图像与原图像之间的质心增量估计平移参数; 然后基于这些估计参数通过模板匹配实现 RST 参数的精确识别; 最后校正图像 $G(x,y)$ 得到 $G'(x,y)$, 并用第 2 节的方法从 $G'(x,y)$ 中提取水印信息 m' , 如图 2 所示。

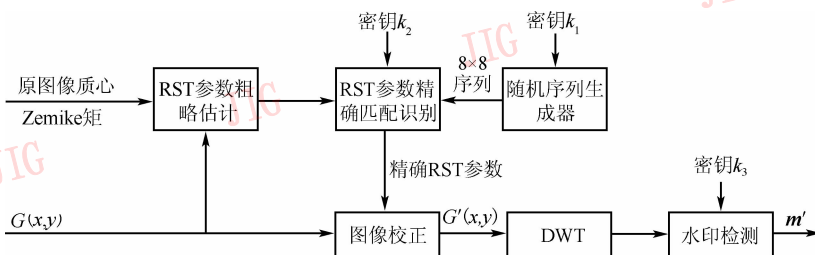


图 2 几何同步和水印检测过程

Fig. 2 Processes of geometrical synchronization and watermark detection

3.1 RST 参数的粗略估计

实际发生几何攻击时,旋转、缩放和平移会伴随发生,对它们的识别会受到彼此之间的相互影响。为了尽可能避免平移对旋转和缩放参数估计的影响,首先将图像进行平移归一化,这样计算出的 Zernike 矩^[7,12]具有平移不变性,从而用 Zernike 矩估计出的旋转和缩放参数也具有平移不变性。设原图像为 $I(x, y)$, 则其质心 (\bar{x}, \bar{y}) 可由下式计算得到。

$$\begin{aligned}\bar{x} &= \frac{m_{10}}{m_{00}} = \frac{\iint xI(x, y) dx dy}{\iint I(x, y) dx dy} \\ \bar{y} &= \frac{m_{01}}{m_{00}} = \frac{\iint yI(x, y) dx dy}{\iint I(x, y) dx dy}\end{aligned}\quad (4)$$

利用 (\bar{x}, \bar{y}) 实现平移归一化后的图像为 $I_1(x, y) = I(x - \bar{x}, y - \bar{y})$; 后面对于 Zernike 矩的计算都是基于归一化后的图像 $I_1(x, y)$ 来进行。

下面仅给出缩放参数和平移参数的估计算法,有关旋转参数的估计参见文献[17]中的算法。

3.1.1 用 Zernike 矩估算缩放参数

假设原图像为 $I(x, y)$ 映射到单位圆时的半径为 R_{or} ^[10,12], 现将其进行缩放(缩放因子为 β)得到 $I^s(x, y)$, 则其映射半径变为 $R_s = \beta R_{or}$ 。根据 Zernike 矩的定义^[10,12]并考虑到实际操作中引入的噪声,可以推得缩放因子的近似值:

$$\hat{\beta}_{nm} = \left(\frac{\|Z_{nm}^s\|}{\|Z_{nm}\|} \right)^{\frac{1}{n+2}}, |m| = n, n = 0, 1, 2, \dots \quad (5)$$

式中, Z_{nm} 和 Z_{nm}^s 分别为缩放前后的第 (n, m) 阶 Zernike 矩。与旋转参数估计类似^[17], 可以用概率密度函数来估计缩放参数,有

$$P(\beta) = \sum_n \sum_m \xi_{nm} P(\beta | n, m), \beta > 0 \quad (6)$$

式中, $P(\beta | n, m) = \delta\{\beta - \hat{\beta}_{nm}\} * G(\beta, \sigma)$, σ 由实验确定;其他参数与估计旋转参数时^[17]的相同。 $P(\beta)$ 最大时所对应的 β 就是所求的缩放因子。

3.1.2 用质心增量估算平移参数

假设对原图像 $I(x, y)$ 向右和向下各平移 Δx 和 Δy , 则有 $I_1(x, y) = I(x - \Delta x, y - \Delta y)$ 。根据式(4)可得平移前后的质心分别为 (\bar{x}_0, \bar{y}_0) 和 (\bar{x}_1, \bar{y}_1) 。在理想状况下,积分区间为无穷大,因此质心的增量满足

$$\Delta x' = \bar{x}_1 - \bar{x}_0 = \Delta x, \Delta y' = \bar{y}_1 - \bar{y}_0 = \Delta y \quad (7)$$

实际上,由于积分区间就是图像的像素所构成的有限区间,所以上述求得的增量只是真实平移量的近似值。

3.2 RST 参数的精确识别

前面估算的旋转、缩放和平移参数可能由于各种误差而偏离真实值,为此需借助于模板进行准确的识别。但既然估计值是在真实值的附近,在进行模板匹配时就可以基于这些估算参数在一个小范围内进行搜索,从而较大幅度地减小搜索的空间,提高搜索效率。这一过程就是由粗到精的几何同步过程。

由于正交小波变换不具有平移、旋转和缩放不变特性,因此在进行模板匹配时,不能直接在小波域通过旋转、缩放和平移来实现,而必须先空域进行旋转、缩放或平移,然后再在小波域检测模板。

3.2.1 旋转参数的精确识别

实际的旋转攻击或校正中,都会同时伴随自动裁剪以保持大小不变,从而有可能使得图像整体上发生向上(或向下)和/或向左(或向右)的少量平移(一般为 1 个像素)。所以在搜索旋转参数的过程中还需要搜索平移参数。

假定已经利用文献[17]的方法估算出旋转角度为 r_0 , 则旋转搜索空间构造为 $S_r = \{r; r = s_r \times k + r_0 - D_r, k \in [0, 2D_r/s_r]\}$ 和 $S_t = \{(x, y); x, y \in \{-1, 0, +1\}\}$ 。其中 s_r 为搜索步长, DA 和 S_r 都为正的常数,并可由实验确定。基于粗估角度 r_0 和小波域模板的旋转参数匹配算法如下:

(1) 初始化搜索角度 r 为 $r_0 - D_r$;

(2) 将 $G(x, y)$ 旋转 $-r$ 度, 并进行裁剪以保持旋转前后大小不变, 得 $G_1(x, y)$;

(3) 搜索平移空间 S_t : 按顺序取其中的任一元素 (x, y) , 将 $G_1(x, y)$ 平移 (x, y) , 检测模板并计算模板相关值;

(4) 如果收敛条件满足, 则算法结束并返回匹配结果, 否则重复第 3 步直至搜索完平移空间 S_t ;

(5) 若搜索完 S_t 仍未收敛, 则将 r 增加 s_r , 重新进行 2~4 步, 直到算法收敛或者搜完旋转参数空间 S_r 。

从以上的匹配算法可知, 搜索的计算复杂度为所需要进行搜索的平均次数, 即 $(2D_r/s_r + 1) \times 9/2$, 它取决于 s_r 和 D_r 的取值。

3.2.2 缩放参数的精确识别

因图像的大小为正整数, 缩放前后即使按原来

的缩放因子进行反向缩放,也有可能造成图像的大小会发生变化。例如,缩放前是 512×512 , 缩小为 $1/10$ 则变为 51×51 , 再放大 10 倍, 图像尺寸变为 510×510 。为了准确检测出模板, 必须使搜索的步长能与 1 像素等价, 如对于 512×512 图像, 搜索步长为 0.02 时等价于 1 个像素。

假定已按 3.1.1 节中的方法估算出了缩放因子 β , 构造缩放参数的搜索空间 $S_s = \{s; s = s_s \times k + \beta_0 - D_s, k \in [0, 2DS/s_s]\}$ 。其中, s_s 为搜索时的步长, s_s 和 D_s 都为正常数, 并可由实验确定。缩放参数匹配算法与旋转参数的匹配算法相似, 去掉空间 S_r 的搜索步骤以及将搜索的空间改为 S_s 即可。根据匹配算法, 搜索的计算复杂度为所需要进行搜索的平均次数, 即 $(2D_s/s_s + 1)$, 它取决于 s_s 和 D_s 的取值。

3.2.3 平移参数的精确识别

假定除平移攻击外没有其他攻击, 或者已经校正或近似校正旋转和缩放参数, 且根据 3.1.2 节中的方法估计出了质心的增量 Δx 和 Δy , 则可构造平移搜索空间为 $S_t = \{(x, y); x = s_t \times k_1 + \Delta x - D_x, y = s_t \times k_2 + \Delta y - D_y, k_1 \in [0, 2D_x/s_t], k_2 \in [0, 2D_y/s_t]\}$ 。其中, s_t 是搜索步长, s_t, D_x 和 D_y 都是正的常数, 并可由实验确定。平移参数匹配算法与旋转参数的相同, 只不过将那儿的搜索空间换成这里的平移搜索空间 S_t 。

从以上的匹配算法可知, 搜索的计算复杂度为所需要进行搜索的平均次数, 即 $(2D_x/s_t + 1) \times (2D_y/s_t + 1)/2$, 它取决于 s_t, D_x 和 D_y 的取值; 每次搜索的计算量主要体现在对于模板序列的检测上。

3.3 RST 联合攻击下 RST 参数的精确识别

对图像实施的几何攻击, 常常会出现旋转、缩放

和平移联合进行的情形, 这对几何同步带来更大的麻烦。由于模板只有一个, 在匹配的过程中这三者会相互牵制, 因此要实现 RST 参数的精确匹配, 必须三者联动搜索才行。

用 Zernike 矩估计旋转和缩放参数的实验中, 发现缩放参数的估计值几乎不受旋转和平移的影响 (参见第 5 节), 而旋转参数的估计值受缩放和平移的影响则相对较大。同时考虑到平移参数必须在校正或近似校正旋转和缩放后才能估计出来, 因此在 RST 联动搜索时, 应该先搜索 S_s , 然后搜索 S_r , 最后才搜索 S_t 。即首先进行反向缩放; 然后对于缩放后的图像进行反向旋转; 接着对反向缩放和旋转后的图像计算质心, 利用 3.1.2 的方法估计平移, 并进行平移搜索; 最后检测模板序列, 计算模板相关值 $\rho_{T,s}$, 并按照前述算法收敛的准则进行判断。如果算法收敛, 则停止搜索, 否则继续上述循环直至收敛或搜索完所有空间为止。平均搜索量是 3 个搜索空间大小的乘积的一半, 每次搜索主要涉及到模板检测。

4 实验结果及分析

在实验仿真中, 采用了 5 幅具有不同纹理特性的 $512 \times 512 \times 8b$ 标准图像, 包括 Barb、Boat、F16、Lena 和 Sailboat。采用 9/7 双正交小波进行 4 层小波分解, 在 $HH_i, HL_i, LH_i (i=3, 4)$ 中基于向量 DWT-HMM 嵌入 60 比特水印, 在小波域 LL_2 子带嵌入模板, 获得嵌入模板和水印后的图像, 如图 3 所示。其中模板嵌入时, 采用了 8×8 的随机序列, 嵌入强度为 $\alpha = 60$ 。



(a) Barb (PSNR=40.26dB) (b) Boat (PSNR=39.74dB) (c) F16 (PSNR=38.83dB) (d) Lena (PSNR=42.72dB) (e) Sailboat (PSNR=39.84dB)

图 3 嵌入模板和水印后的图像

Fig. 3 Image embedded with the template and watermark

考虑到旋转和缩放参数估计公式的约束、估计精度和辅助信息量之间的折衷, 在实验仿真时只采用了 $(0, 0)$ 、 $(2, 2)$ 、 $(3, 3)$ 和 $(4, 4)$ 这 4 个 Zernike

矩。对于 512×512 的灰度图像, 像素值不超过 255, 而实验中只以半径为 $96 (= 256 \times 3/8)$ 圆内的像素来计算 Zernike 矩, 则每个矩最多需要 $23 (=$

$\log_2(2^8 \times 2^9 \times 2^9/2^3)$ 个比特。由于第 $(0, 0)$ 阶 Zernike 矩的虚部永远为 0, 因此 4 个矩的实部和虚部共需要的比特数最多不超过 $161 (= 7 \times 23)$ 个比特。另外, 原图像质心坐标 (\bar{x}, \bar{y}) 各用 9 个, 一共 18 个比特已经足够了。综上可知, 辅助信息量与原图像比特数的比率在 10^{-5} 数量级。

(1) 旋转和缩放参数估计性能

利用 Lena 图像进行实验, 用这 4 个矩来估计

的旋转参数和缩放参数的性能如图 4 所示。其中, 图 4(a) 为在不同组合攻击下旋转角度绝对估计误差与真实旋转角度之间的性能曲线, 图 4(b) 为在不同组合攻击下缩放比例绝对估计误差与真实缩放比例之间的性能曲线。由图可知, 旋转和缩放参数的估计误差都很小, 尤其是缩放参数的估计。

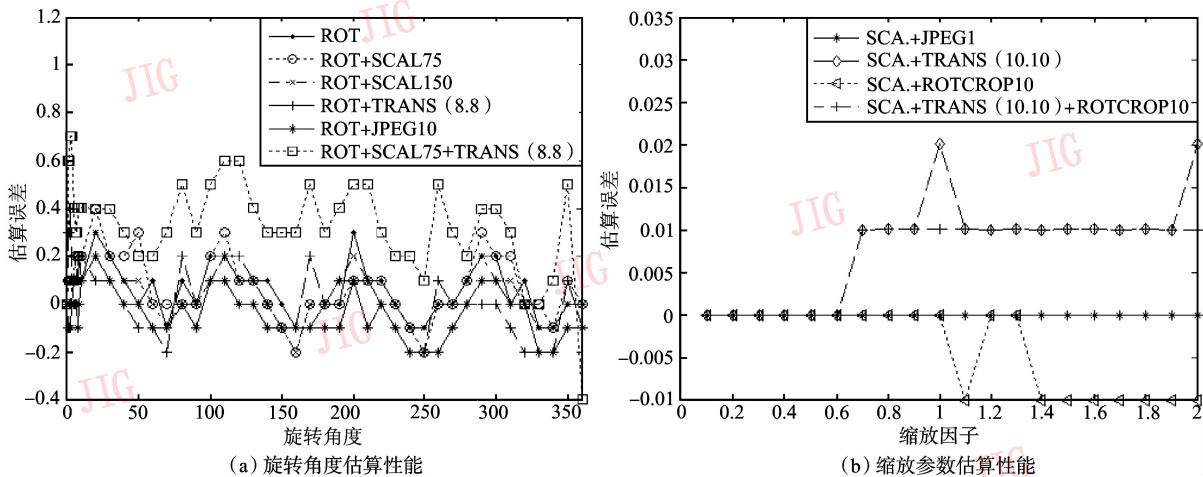


图 4 用 Zernike 矩估算旋转和缩放参数的性能

Fig. 4 Performance of rotation and scaling estimation with Zernike moments

(2) 抵抗 StirMark 4.0 攻击性能

用 StirMark 4.0 平台对图 3 中嵌入模板和水印后的图像进行攻击, 然后用本文提出的几何同步算法来精确识别 RST 参数。RST 搜索空间的设置如下: (1) S_r 空间的 $D_A = 0.3$ 和 $s_r = 0.1$, (2) S_s 空间的 $D_s = 0.01$ 和 $s_s = 0.002$, (3) S_t 空间的 $D_x = D_y = 1$ 和 $s_t = 1$; 取虚警概率为 1×10^{-6} , 可求得 T_p 为 0.59, 则相应的实验结果如表 1 所示。其中, Rot._Crop 在 Matlab 6.5 中实现, 指先对图像进行旋转然后进行裁剪以保持旋转前的大小; MedianCut 的模板为 $2 \times 2, 3 \times 3, 4 \times 4, 5 \times 5, 7 \times 7$ 这 5 种; X_Shearing、Y_Shearing、XY_Shearing 和 Gen._Shearing 的参数分别为 $1_0.01_0_0_1_0, 1_0_0_0.01_1_0, 1_0.01_0_0.01_1_0$ 和 $1.013_0.008_0.011_1.008$ 。

由表 1 的结果可知, 本算法能较好地抵抗 StirMark 4.0 平台的各种攻击。值得指出的是, 在多种 MedianCut 模板攻击下仍然能够无误地达到模板匹配和水印检测, 这说明本算法设计的模板本身具有较强的鲁棒性, 不会被轻易地除去。

表 1 在 StirMark 4.0 平台攻击下的水印检测结果

Tab.1 Results of watermark detection under StirMark attacks

攻击	图像				
	Barb	Boat	F16	Lena	Sailboat
Rot._Crop * (°)	-20 ~ 20	-20 ~ 20	-20 ~ 20	-20 ~ 20	-20 ~ 20
Scaling	≥ 0.3	≥ 0.3	≥ 0.3	≥ 0.3	≥ 0.3
X-Shearing	OK	OK	OK	OK	FAIL
Y-Shearing	OK	OK	OK	OK	OK
XY-Shearing	FAIL	FAIL	OK	OK	FAIL
Gen._Shearing	OK	OK	OK	OK	FAIL
AddNoise	1 ~ 2	1 ~ 2	1 ~ 7	1 ~ 3	1 ~ 3
JPEG QF	19 ~ 100	15 ~ 100	16 ~ 100	18 ~ 100	19 ~ 100
MedianCut *	$\leq 7 \times 7$	$\leq 5 \times 5$	$\leq 5 \times 5$	$\leq 3 \times 3$	$\leq 5 \times 5$
Sharpening	OK	OK	OK	OK	OK

(3) 抗 RST 联合攻击性能

对嵌有模板和水印的 Lena 图像进行联合攻击: 将图像放大 1.2 倍, 然后向右和向下各平移 5 个像素, 接着旋转 10° (含自动裁剪), 最后进行 $QF = 20$ 的深度 JPEG 压缩攻击, 生成联合攻击图像, 如图 5(a) 所示。采用 (2) 中给出的 RST 搜索空间参



图 5 联合攻击图像及其校正后的图像

Fig.5 Image undergone with joint attacks and its corrected version

数,利用由粗到精的几何同步算法,得到 RST 的精确匹配参数:缩放参数为 1.20,旋转参数为 10.1;水平和垂直平移分别为 $\Delta x = 4, \Delta y = 3$ 。根据这些参数进行图像校正,得到校正后的图像,如图 5(b)所示。最后,水印可以无误地从校正后的图像中检测出来。对其他 4 幅图像都进行类似的操作,结果都能无误地检测出水印信息,相应的模板匹配和水印检测结果如表 2 所示。由表 2 可知,本文算法能很好地抵抗深度 JPEG 压缩和 RST 的联合攻击,表明该算法具有较好的鲁棒性能。

表 2 在 S(1.2) + T(5,5) + R(10) + JPEG(20) 联合攻击下的模板匹配和水印检测结果

Tab.2 Template matching and watermark detection under the joint S(1.2) + T(5,5) + R(10) + JPEG(20) attack

参数		图像				
		Barb	Boat	F16	Lena	Sailboat
缩放	估计值	1.2	1.2	1.2	1.2	1.2
	匹配值	1.2	1.2	1.2	1.2	1.2
旋转	估计值	10.7	10.3	9.7	9.6	9.7
	匹配值	10.1	10.1	10.1	10.1	10.1
平移	(4,3)	(4,3)	(4,3)	(4,3)	(4,3)	
模板相关值	0.875	0.875	0.875	0.875	0.875	
水印检测结果	OK	OK	OK	OK	OK	

(4) 本文算法性能分析与比较

在单项 RST 攻击时,本文提出的由粗到精的搜索算法具有较高的搜索效率。若采用(2)中给出的 RST 搜索空间参数,则根据 3.2 节中给出的计算复杂度公式可知,对于旋转、缩放和平移所需的平均搜索次数如表 3 所示。然而,大量的实验结果表明单项缩放攻击时缩放参数估计得相当准确,直接采用估计值就完全可以成功地匹配到模板和正确地检测

出水印信息,因此实际的缩放攻击只需要 1 次匹配即可完成。

表 3 单项 RST 攻击时的平均搜索次数

Tab.3 Average searching time under separate RST attack

次数	参数		
	旋转	缩放	平移
31.5 (=7×3×3/2)	5.5 (=(0.02/0.002+1)/2)	4.5 (=3×3/2)	

由表 3 可知,采用由粗到精的策略平均搜索量是相对较小的。如果采用穷举搜索的话,对于 512×512 的灰度图:(1)对于旋转参数的估计,如果图像旋转 10°后以 0.1°的精度进行搜索,平均需要 105(=21/0.1/2)次搜索;(2)对于缩放参数的估计,如果仅仅将图像缩放到原来大小的 1.04 倍(大小增加了 20 个像素),以 1 个像素精度进行搜索,平均需要 20.5(=41/2)次搜索;(3)对于平移参数的估计,由于无法确定平移方向,因此以 1 个像素精度进行搜索时,平均需要 512×512/2 次搜索。另外,Alghoniemyz 在文献[18]中给出了一种利用小波极值矩并结合空域模板来估计旋转和缩放参数的方法,本文方法在缩放参数估计方面结果比文献[18]的结果要好,在旋转参数估计方面两者相当,具体比较参见表 4 和表 5。

由于缩放参数估计得很准,因此联合攻击的计算复杂度取决于旋转空间和平移空间的大小及其搜索步长。对于(3)中给出的参数,联合搜索 S_r 和 S_t 的总次数为 49.5(=11×3×3/2)次。相对于文献[11],那里为了搜索并获得仿射变换 a, b, c 和 d 值时就需要将 0 到 π 的范围分为 90 个等角度的区间,且没有解决平移搜索问题,因此本文采用的这种由粗到精的方式相对来说在一定程度上减小了搜索量,提高了几何同步的效率。

表 4 不同算法旋转参数估计比较

Tab.4 Performance comparison for rotation estimation with different algorithms

图像	算法	角度				
		-0.5°	-1°	-2°	0.5°	2°
Camera	文献[18]	无	-0.93	-1.989	0.415	1.978
	本文算法	无	-1.00	-2.000	0.500	1.800
F16	文献[18]	-0.507	-0.89	-1.88	0.507	无
	本文算法	-0.500	-1.00	-1.80	0.500	无

注:“无”表示文献[18]中所没有列出的。

表 5 不同算法缩放参数估计比较

Tab. 5 Performance comparison for scaling estimation with different algorithms

图像	算法	缩放(倍)					
		0.5	0.75	0.90	1.10	1.50	2.00
Camera	文献[18]	0.472	0.745	无	无	1.483	1.948
	本文算法	0.500	0.750	无	无	1.500	2.000
Fl6	文献[18]	无	0.788	0.914	1.104	1.506	无
	本文算法	无	0.750	0.900	1.100	1.500	无

注:“无”表示文献[18]中所没有列出的。

5 结 论

提出了一种由粗到精的几何同步方法,以抵抗图像所受的各种几何攻击。首先用平移归一化图像的 Zernike 矩估计旋转和缩放参数,并用校正旋转和缩放后图像的质心增量来估计平移参数;然后利用小波域模板匹配精确识别 RST 参数;最后基于这些参数校正图像所受的几何攻击。采取由粗到精的搜索策略可以在一定程度上降低搜索空间,提高搜索效率。实验仿真结果表明,结合基于向量 DWT-HMM 的水印嵌入和检测算法,该算法能有效抵抗 StirMark 平台的多种单项攻击(如 RST、Shearing、JPEG 压缩、加噪、中值滤波等)和联合攻击(如 RST 和 JPEG 压缩联合),因而具有较好的鲁棒性能。

参考文献 (References)

- Hartung F, Kutter M. Multimedia watermarking techniques [J]. Proceedings of IEEE, 1999, **87**(7): 1079 ~ 1107.
- Cox I J, Miller M L, Bloom J A. Digital Watermarking [M]. San Francisco, California, USA: Morgan Kaufmann Publishers, 2001.
- Bas P, Chassery J M, Macq B. Geometrically invariant watermarking using feature points [J]. IEEE Transactions on Image Processing, 2002, **11**(9): 1014 ~ 1028.
- Deguillanume F, Voloshynovskiy S, Pun T. A method for the estimation and recovering from general affine transforms in digital watermarking applications [J]. Proceedings of SPIE, 2002, **4675**: 313 ~ 322.

- Kang X, Huang J, Shi Y Q, *et al.* A DWT-DFT composite watermarking scheme robust to both affine transform and JPEG compression [J]. IEEE Transactions on Circuit and Systems for Video Technology, 2003, **13**(8): 776 ~ 786.
- O' Ruanaidh J J K, Pun T. Rotation, scale and translation invariant spread spectrum digital image watermarking [J]. IEEE Transactions on Signal Processing, 1998, **66**(3): 303 ~ 317.
- Kim H S, Lee H-K. Invariant image watermark using Zernike moments [J]. IEEE Transactions on Circuit System and Video Technology, 2003, **13**(8): 766 ~ 775.
- Xin Y, Liao S, Pawlak M. Multibit geometrically robust image watermark based on Zernike moments [A]. In IEEE Proceedings of the 17th International Conference on Pattern Recognition (ICPR'04) [C], Cambridge, UK, 2004: 861 ~ 864.
- Tang C-W, Hang H-M. A featured-based robust digital image watermarking scheme [J]. IEEE Transactions on Signal Processing, 2003, **51**(4): 950 ~ 959.
- Teague M. Image analysis via the general theory of moment [J]. Journal on Optical Society of America, 1980, **70**(8): 920 ~ 930.
- Pereira S, Pun T. Robust template matching for affine resistant image watermarks [J]. IEEE Transactions on Image Processing, 2000, **8**(6): 1123 ~ 1129.
- Khotanzad A, Hong Y H. Invariant image recognition by Zernike moments [J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 1990, **12**(5): 489 ~ 497.
- Ni J, Zhang R, Huang J. HMM-based in wavelet domain robust multibit image watermarking algorithm [A]. In: Proceedings of International Workshop on Digital Watermarking 2005 [C]. Siena, Italy, 2005: 110 ~ 123.
- Crouse M S, Nowak R D, Baraniuk R G. Wavelet-based statistical signal processing using hidden Markov models [J]. IEEE Transactions on Signal Processing, 1998, **46**(4): 886 ~ 902.
- Do M N, Vetterli M. Rotation invariant texture characterization and retrieval using steerable wavelet-domain Hidden Markov Models [J]. IEEE Transactions on Multimedia, 2002, **4**(4): 517 ~ 527.
- Petitcolas F A P. Watermarking schemes evaluation [J]. IEEE Signal Processing, 2000, **17**(5): 58 ~ 64.
- Kim W-Y, Kim Y-S. Robust rotation angle estimator [J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 1999, **21**(8): 768 ~ 773.
- Alghoniemy M. Multimedia distribution [D]. Minnesota, USA: University of Minnesota, 2001.