基于改进的不变质心和小波域的鲁棒数字图像水印方法

夏 嵬[1] 鲁宏伟[1] 谢长生[1] 赵小厦[2]
(华中科技大学计算机科学与技术学院 武汉 430074)[1] (华南师范大学计算机学院 广州 510631)[2]

摘 要 利用图像不变质心在图像中的相对位置对平移、旋转和缩放的不变性,提出了一种抗几何攻击的图像盲水印算法。算法首先根据水印比特的长度自适应地对原始图像进行特定级的小波分解,并修改某些相对稳定的最低一级的低频子图的小波系数,通过将修改后的系数进行小波重构来嵌入水印。接下来以含水印图像的基于改进的不变质心的不变特征矩阵为基础,与Rijndael加密技术相结合,生成相关的二值逻辑表作为密钥向第三方认证,达到版权保护的目的。该算法在提取水印时不需要原始载体图像和原始水印。实验结果表明,该算法时间复杂度低,能有效抵抗JPEG压缩、裁剪、噪声等常规攻击以及平移、旋转、缩放等几何攻击。

关键词 不变质心,几何攻击,小波分解,不变特征矩阵,Rijndael加密
中图法分类号 TP391 **文献标识码** A

Robust Image Watermarking Based on Improved Invariant Centroid and Wavelet Domain

XIA Wei[1] LU Hong-wei[1] XIE Chang-sheng[1] ZHAO Xiao-sha[2]
(College of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074, China)[1]
(College of Computer, South China Normal University, Guangzhou 510631, China)[2]

Abstract A geometrically robust blind watermarking algorithm was proposed using translation, rotation and scaling invariant property of relative coordinate of the invariant centroid. With certain level wavelet decomposition according to the length of the watermark bits, after modifying some selected coefficients in the lowest frequency of the last level for its robustness to the interference, the modified coefficients were applied to obtain the watermarked image by wavelet reconstruction. With the improved invariant centroid based characteristic matrix and the Rijndael encryption, a related binary logical table was produced. As the secret key, the table was used to apply to the third party for copyright protection. This arithmetic can extract the watermarking without the original carrier image and the original watermarking. Experimental results show its low time complexity and robustness to the common attacks such as JPEG compression, cropping and added noise, as well as the geometric attacks such as translation, rotation and scaling.

Keywords Invariant centroid, Geometric attacks, Wavelet decomposition, Invariant characteristic matrix, Rijndael encryption

随着数字全球化技术和因特网的发展,各种形式的多媒体数字产品纷纷在网络上被复制和传播。然而,便利性和不安全性是并存的,这些资源在给使用者提供方便的同时,也给了盗版者以可乘之机。数字水印技术作为多媒体数据强有力的版权保护工具,一直受到人们的广泛关注。在数字水印技术中,旋转、平移和缩放等几何攻击能够破坏水印检测的同步性,微小的几何攻击就可能使得水印检测失败。人们已经提出了几种新的数字水印模式[1-3],但在抗几何攻击方面还没有什么大的突破。因此,设计能够抵抗几何攻击的水印算法,成为水印技术研究的一个新热点。一个好的数字水印算法应该综合考虑水印的不可见性、鲁棒性以及嵌入容量等方面。目前,抗几何攻击的水印算法主要有基于不变矩的方法和基于图像特征的方法。

基于不变矩理论,Kim等[4]通过修改低于5阶的Zernike矩,结合图像归一化,设计了具有几何不变性的数字水印。Li等[5]利用伪Zernike矩的幅度具有旋转不变的性质,提出一种抗几何攻击的水印算法。这类算法利用不变矩的特点,结合归一化的思想,获得了较好的抗几何攻击性能。它由于计算时利用图像全局信息,因此对于裁剪攻击不具备鲁棒性。绝大多数水印算法都把图像作为整体,全局性嵌入水印,没有考虑到重要的视觉目标区域,因此有很大的局限性。沃焱等[6]通过对Zernike矩正则化后进行筛选,提出了一种改进的基于Zernike矩的抗几何攻击的水印方法,并通过对图像进行同心环分块来加强水印对裁剪攻击的鲁棒性。能抵抗几

到稿日期:2010-05-25 返修日期:2010-09-05 本文受国家自然科学重点基金(60933002),国家"863"重大专项计划(2009AA01A402),武汉市晨光计划(201050231073)资助。

夏 嵬(1979-),男,博士生,主要研究方向为信息安全,E-mail:xw7932@126.com;鲁宏伟(1964-),男,博士,教授,主要研究方向为网络安全;谢长生(1957-),男,教授,博士生导师,主要研究方向为网络安全高密度硬盘与光盘关键技术研究、海量信息存储理论;赵小厦(1982-),女,硕士生。

何攻击的不变矩一般有一个缺点，即构造复杂、算法复杂度高，这使得整个水印系统的效率会打折扣。

对于基于图像特征的方法，寻找到适用于水印算法的简易实用的图像特征是一个很具有挑战性的问题。Liu[7]提出了基于图像局部特征点检测的抗 RST 攻击鲁棒水印算法，其缩放比例为 80%到 120%，但旋转角度只有 12°，抗旋转攻击能力有待提高。Ji 等[8]采用分水岭法对图像进行区域分割，将水印扩频嵌入到各个分割区域[9]，但分水岭法普遍存在过度分割问题，算法的应用存在局限性[10]。还有一些利用图像归一化思路抗几何攻击的方法[11]，但这些方法对裁剪鲁棒性较差。本文结合高可靠性的 Rijndael 加密，提出了一种基于改进的不变质心和小波域的数字水印。它可以根据水印的容量自适应地在某些相对稳定的低频域小波系数中嵌入水印，并利用由一系列改进的不变质心构造的不变特征矩阵以及与水印相关的二值表来达到版权认证的目的，在保证能抵抗各种常见攻击和几何攻击的情况下，使水印的嵌入容量和不可见性都有了保障。该算法嵌入实际的比特序列，在提取水印时不需要原始载体图像和原始水印信息。

1 图像的不变质心的提取、性质及改进

对于一幅大小为 $N\times M$ 的图像 $f(x,y)$，基于半径为 R 的不变质心的求取步骤如下。

第一步　计算出整个图像的质心$(\bar{x},\bar{y})$，并将质心$(\bar{x},\bar{y})$作为求不变质心的基点$(\bar{x}_B,\bar{y}_B)$，即$(\bar{x}_B,\bar{y}_B)=(\bar{x},\bar{y})$。不变质心的计算公式如下：

$$\bar{x}=\sum_{x=0}^{N-1}\sum_{y=0}^{M-1}xf(x,y)/\sum_{x=0}^{N-1}\sum_{y=0}^{M-1}f(x,y) \tag{1}$$

$$\bar{y}=\sum_{x=0}^{N-1}\sum_{y=0}^{M-1}yf(x,y)/\sum_{x=0}^{N-1}\sum_{y=0}^{M-1}f(x,y) \tag{2}$$

第二步　按照第一步的方法，计算出以$(\bar{x}_B,\bar{y}_B)$为圆心、R 为半径的圆形图像区域的质心，公式如下：

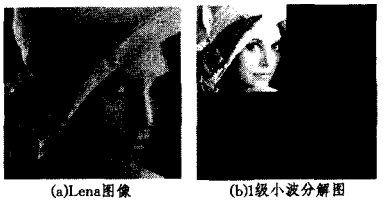
$$\bar{x}_R=\sum_{(x-\bar{x}_B)^2+(y-\bar{y}_B)^2\leqslant R^2}xf(x,y)/\sum_{(x-\bar{x}_B)^2+(y-\bar{y}_B)^2\leqslant R^2}f(x,y) \tag{3}$$

$$\bar{y}_R=\sum_{(x-\bar{x}_B)^2+(y-\bar{y}_B)^2\leqslant R^2}yf(x,y)/\sum_{(x-\bar{x}_B)^2+(y-\bar{y}_B)^2\leqslant R^2}f(x,y) \tag{4}$$

第三步　如果$(\bar{x}_R,\bar{y}_R)$和$(\bar{x}_B,\bar{y}_B)$重合，那么$(\bar{x}_R,\bar{y}_R)$就是所求的不变质心；如果$(\bar{x}_R,\bar{y}_R)$和$(\bar{x}_B,\bar{y}_B)$不重合，那么将$(\bar{x}_R,\bar{y}_R)$设置为$(\bar{x}_B,\bar{y}_B)$，回到第二步，继续循环执行第二步和第三步，直到$(\bar{x}_R,\bar{y}_R)=(\bar{x}_B,\bar{y}_B)$，得出不变质心$(\bar{x}_R,\bar{y}_R)$为止。

我们把不变质心的相对位置坐标定义为$(\bar{x}_R/M,\bar{y}_R/N)$。当 $f(x,y)$受到攻击时，用式(1)和式(2)求出的常规意义下的质心在图像中的相对位置会有不同程度的偏移，而不变质心对于攻击，特别是平移、旋转、缩放等几何攻击具有较好的鲁棒性，攻击前后不变质心在图像中的相对位置基本不会发生变化。虽然对于不同的半径 R，$(\bar{x}_R,\bar{y}_R)$会不相同，但如果固定 R，$(\bar{x}_R,\bar{y}_R)$对于攻击是具有相当程度稳定性的。

用以上方法得出的不变质心对于缩放的鲁棒性还可以进一步加强。可以对 $f(x,y)$进行 L 级小波分解，进行一级小波分解后，图像分为 4 个子图，而每一级分解得到的低频子图又可以继续进行二级小波分解，依此类推。一种改进的方法就是对分解后最后一级低频逼近子灰度图 $f_L(x,y)$求基于同比半径 $R/2^L$ 下的不变质心。对于 $f_L(x,y)$，没有使用整个图像，而只是使用了子图包含的信息，这样得出的不变质心对裁剪的鲁棒性也得到了加强。L 越大，鲁棒性就越好。图 1 是对 128×128 的 256 灰度级 Lena 图像进行 1 级小波分解的结果。



(a)Lena图像　　(b)1级小波分解图

图 1　Lena 图像 1 级小波分解图

将 $f(x,y)$设为 Lena 图像，在半径 $R=30$、分解级数 $L=1$ 的条件下做个实验。在没有攻击的情况下，可以求出$(\bar{x}_R,\bar{y}_R)$以及 $f_L(x,y)$在同比半径为 15 时的不变质心$(\bar{x}_R',\bar{y}_R')$，进而分别得出两个质心的相对位置坐标(p_1,p_2)以及(p_1',p_2')。将 $f(x,y)$进行 25%的裁剪后，可以重新求得两个质心的相对位置坐标(p_3,p_4)以及(p_3',p_4')，相对位置偏移量$(|p_3-p_1|,|p_4-p_2|)$以及$(|p_3'-p_1'|,|p_4'-p_2'|)$分别为(0.0147,0.0174)和(0.0124,0.0143)。对于因子为 2 的缩放攻击，将半径设为 60，同比半径相应为 30，用同样方法可以求得两个相对位置偏移量分别为(0.0031,0.003)和(0.0016,0.0018)。可以看出，改进的方法得到的不变质心的相对偏移量较小。

我们根据这个特点可以提取出图像的某种量化的不变特征，建立一个基于此不变特征的数学模型。在嵌入和提取水印时，可以利用这个特征达到水印的鲁棒性效果。下面在介绍水印算法的过程中将对此做详细的讨论。

2 抗几何攻击的鲁棒水印算法

在这里，假设大小为 $N\times M$ 的图像 $f(x,y)$为原始载体图像，而水印图像是一个有意义的二值图像 $W(x,y)$，大小为 $N_1\times M_1$ $(N_1\leqslant N,M_1\leqslant M)$。

2.1 水印的嵌入

2.1.1 基于改进的不变质心的不变特征矩阵

对图像 $f(x,y)$进行 L 级小波分解，可以求出分解后最后一级低频逼近子灰度图 $f_L(x,y)$的质心$(\bar{x},\bar{y})$以及质心到图像 $f_L(x,y)$上下左右 4 条边界线段的 4 个距离，将这 4 个距离按从小到大的顺序依次记为 D_1,D_2,D_3 和 D_4。所有 $f_L(x,y)$的像素点到$(\bar{x},\bar{y})$都有一个距离，不难求出其中最大距离为 $R_l=\sqrt{D_3^2+D_4^2}$。

为了获得良好的不变性，就要使求不变质心时所使用的区域都为圆形，也就是所有的圆形区域都严格包含在整个子灰度图像区域的范围内。所以必须首先保证以质心$(\bar{x},\bar{y})$为圆心的圆形区域不超出整个子灰度图像区域。为此，我们选取的所有圆的半径都应该不大于 D_1，否则圆区域就会有部分落在图像外，使得结果产生偏差。

作为抵抗攻击的关键，不变特征的提取和构造至关重要。不变特征在攻击前后变化越小，水印的鲁棒性也就越好。对于平移和旋转攻击，攻击前后图像的尺寸未发生变化，而对于

缩放攻击，如果缩放因子为 α，则缩放前后图像面积（像素数量）的比为 $1/\alpha^2$。根据这些特点，对于特定的半径，我们引入一个认为在几何攻击下相对稳定的不变量。假设选择的半径为 R，设 $\eta=R/D_1$（$0<\eta\leqslant 1$），我们将求得的不变质心 $(\bar{x}_R,\bar{y}_R)$ 与 $(\bar{x},\bar{y})$ 之间的距离与 R_l 的比值定义为 η 水平下的不变量，记为：

$$I_\eta=\sqrt{(\bar{x}_{\eta D_1}-\bar{x})^2+(\bar{y}_{\eta D_1}-\bar{y})^2}/R_l \tag{5}$$

根据假设，不变质心是在子灰度图像内部的，所以 $(\bar{x}_R,\bar{y}_R)$ 与 $(\bar{x},\bar{y})$ 之间的距离小于 R_l，即 $0\leqslant I_\eta<1$。下面以此为基础来构造图像的不变特征矩阵，步骤如下：

第一步，确定 η 的范围。由于在求不变质心的过程中，如果求出的不变质心 $(\bar{x}_{\eta D_1},\bar{y}_{\eta D_1})$ 和 $(\bar{x},\bar{y})$ 不重合，中间每次求出的质心都会发生偏移。这样，如果 η 值太大，可能会造成半径为 ηD_1 的圆形区域超出整个图像区域。因此可以适当选择一个步长 $\triangle\eta$，使 η 从 1 开始逐步递减 $\triangle\eta$，对每一个 η 水平值求不变质心。如果中间求出的质心对于前面的质心产生偏移，而且求出的质心到图像 4 个边界线段的最小距离小于 ηD_1，则将 η 继续递减 $\triangle\eta$，直到求出不变质心的过程中，所有半径为 ηD_1 的圆都在图像内为止。记此时的 η 为 η'，并将 η 的取值范围定为 $0<\eta\leqslant\eta'$。

第二步，对于特定的 η，将 I_η 转换为二进制形式后，取小数点后的最高 k 位（$k\geqslant 1$）来构造和水印图像大小相同的不变特征矩阵，也就是要取 $\lceil N_1\times M_1/k\rceil$（$\lceil x\rceil$ 表示不小于 x 的最小整数）个不同的 η 值来求不变量 I_η。为此，以 $(\bar{x},\bar{y})$ 为圆心，作 $\lceil N_1\times M_1/k\rceil$ 个同心圆，将 $\eta' D_1$ 为半径的圆形区域等面积地划分为一个圆形区域和 $\lceil N_1\times M_1/k\rceil-1$ 个圆环区域。不难求出这些同心圆的半径分别为：

$$R_n=\sqrt{n/(\lceil N_1\times M_1/k\rceil)}\,\eta' D_1$$
$$(n=1,2,\cdots,\lceil N_1\times M_1/k\rceil) \tag{6}$$

由此可以得出所需的 $\lceil N_1\times M_1/k\rceil$ 个不变量：

$$I_{R_n/D_1}=I_{\eta'\sqrt{n/(\lceil N_1\times M_1/k\rceil)}}\ (n=1,2,\cdots,\lceil N_1\times M_1/k\rceil) \tag{7}$$

将这些不变量二进制化后都取小数点后的最高 k 位，得到 $\lceil N_1\times M_1/k\rceil$ 个 k 位二进制串。最后将这些二进制串合并，得到一个大的二进制串 S。取这个大的二进制串的前 $N_1\times M_1$ 位，便可组成一个大小为 $N_1\times M_1$ 的二值矩阵 A，每一位二进制位依先行后列的顺序作为这个矩阵的一个元素。根据前面的介绍，$I_{\eta'\sqrt{n/(\lceil N_1\times M_1/k\rceil)}}$ 在几何攻击下是具有稳定性的。可以把这个二值矩阵定义为图像 $f(x,y)$ 的 L 级基于不变质心的不变特征矩阵。如果用“F”表示求不变特征矩阵的过程，则整个过程可以简单表示如下：

$$A=F(f,L,N_1,M_1,\eta',k) \tag{8}$$
$$A(i,j)=S(i\times M_1+j)(0\leqslant i<N_1,0\leqslant j<M_1) \tag{9}$$

可以看出，对 I_η 进行二进制编码后，小数点后的高位由于攻击而改变的概率比低位要小一些。也就是说，k 越小，得到的不变特征矩阵越稳定，抗攻击能力越强。但另一方面，$\lceil N_1\times M_1/k\rceil$ 增大，计算开销会加大。

2.1.2 基于小波域的水印的嵌入算法

对于给定的 $N\times M$ 的载体图像 $f(x,y)$ 和 $N_1\times M_1$ 的二值水印图像 $W(x,y)$，用“min”表示取最小值函数，则小波分解级数 L 可按如下条件进行设置：

$$L\leqslant\lfloor\log_2(\min(N/N_1,M/M_1))\rfloor \tag{10}$$

$\lfloor x\rfloor$ 表示不大于 x 的最大整数。分解级数越高，鲁棒性越好，但分解和重构时间加长，计算量加大。分解后得到的子图中，高频细节子图主要包含了丰富的纹理，所含能量小，容易受外界干扰，而低频子图包含了图像的大部分信息，可嵌入大量水印。本算法把水印加在最后一级低频逼近子灰度图 $f_L(x,y)$ 中，通过修改逼近子图小波系数 FA_L，将修改后的系数进行小波反变换来嵌入水印，从而得到含水印图像 $\hat{f}(x,y)$。根据前面的讨论，$\hat{f}(x,y)$ 经过 L 级小波分解后，用低频子图 $\hat{f}_L(x,y)$ 求得的不变量 I 对平移、旋转、缩放等几何攻击也是具有稳定性的，所以在这些攻击下，认为它的基于不变质心的不变特征矩阵也具有相对稳定性。由此，我们可以实现水印的鲁棒性。水印的嵌入过程可用如下公式表示：

$$FA_L'(i,j)=FA_L(i,j)+\alpha W(i,j) \tag{11}$$
$$\hat{A}=F(\hat{f},L,N_1,M_1,\eta',k) \tag{12}$$
$$key(i,j)=RD(\hat{A}(i,j)\oplus W(i,j),k) \tag{13}$$

式中，“α”表示水印嵌入强度，经过水印嵌入后的逼近子图小波系数为 FA_L'，“$\oplus$”表示按位异或运算。“RD”表示用构造特征矩阵所选择的位数 k 作为密钥进行 Rijndael 加密[12]的算法，可加强水印的安全性。$key(i,j)$ 是与水印相关的二值逻辑表。在生成二值逻辑表时，为保证其可靠性，使用了密码学中常用的 HASH 函数。可将 $key(i,j)$，L，η' 和 k 作为密钥向第三方申请，以获得原作品版权[13]。

2.2 水印的提取

水印的提取是嵌入的逆过程。将含水印图像 $\hat{f}'(x,y)$（可能受到过攻击）进行 L 级小波分解，用最后一级低频逼近子灰度图 $\hat{f}'_L(x,y)$ 以及提取出的 η' 和 k 求出不变特征矩阵 A'，利用二值逻辑表 $key(i,j)$ 和 k 进行解密和异或运算来提取水印 $W^*(i,j)$，水印的提取过程不需要原始载体图像。设 Rijndael 解密运算为 $\underline{RD}$，则水印的提取过程可表示如下：

$$A'=F(\hat{f}',L,N_1,M_1,\eta',k) \tag{14}$$
$$W^*(i,j)=\underline{RD}(key(i,j),k)\oplus A'(i,j) \tag{15}$$

3 实验与分析

图 2 是用 128×128 的 256 灰度级 Lena 图像为载体，64×64 大小的二值图像为水印图像在 $L=1$，$\alpha=0.5$，提取位数 $k=5$ 的条件下的实验结果。图 2(a) 是原始载体图像，图 2(b) 是原始二值水印图像，图 2(c) 和图 2(d) 分别是嵌入水印后的图像和提取出的水印。可以看出在水印嵌入量很大时，嵌入水印后图像质量没有下降，兼顾了水印的不可见性和水印容量。另一方面，提取出的水印清晰可辨，表明水印的嵌入和提取算法是有效的。

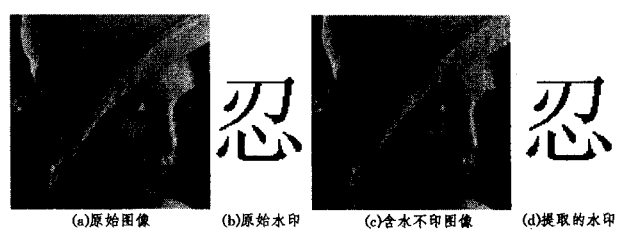
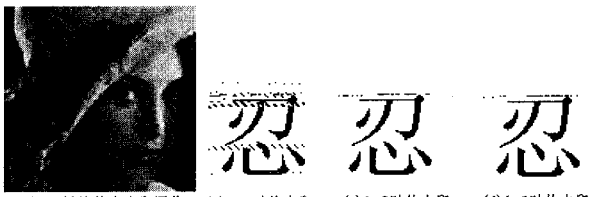


图 2 水印嵌入和提取实验结果

为验证算法的鲁棒性，对含水印图像在 $L=1$，提取位数 k 为 5，3 和 1 的条件下分别进行各种攻击，包括 JPEG 压缩、裁剪、高斯噪声攻击以及平移、旋转、缩放等几何攻击。

3.1 JPEG 压缩攻击

图 3 是对加水印图像进行质量因子为 10% 的 JPEG 压缩攻击的实验结果（质量因子是一个 0 到 1 之间的数，质量因子越小，图像受攻击越严重，图像质量也越差）。图 3(a)是进行压缩后的含水印图像，图 3(b)－(d)分别是在 k 为 5，3 和 1 时从压缩后的含水印图像中提取出的水印图像。即使质量因子只有 10%，提取出的水印图像依然很容易分辨，所以可以认为本算法对 JPEG 压缩攻击具有鲁棒性。

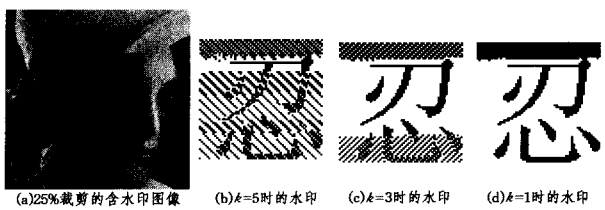


(a)10%压缩的含水印图像　(b)k=5时的水印　(c)k=3时的水印　(d)k=1时的水印

图 3　水印抗 JPEG 压缩攻击的结果

3.2 裁剪攻击

图 4 是对加水印图像中心进行 25% 的裁剪攻击（裁剪区域的长和宽分别是含水印图像长和宽的 1/2）的实验结果。图 4(a)是裁剪后的含水印图像，图 4(b)－(d)分别是在 k 为 5，3 和 1 时相应提取出的水印图像。从结果可以看出本水印算法对裁剪攻击具有鲁棒性。

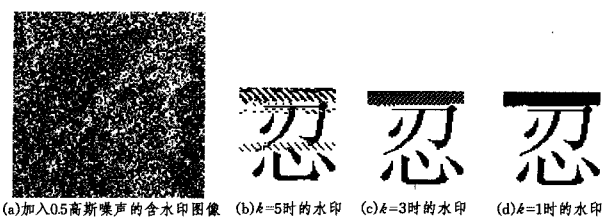


(a)25%裁剪的含水印图像　(b)k=5时的水印　(c)k=3时的水印　(d)k=1时的水印

图 4　水印抗裁剪攻击的结果

3.3 高斯噪声攻击

图 5 是对含水印图像加入 0.5 的高斯噪声进行攻击的实验结果。图 5(a)是加入噪声后的含水印图像，图 5(b)－(d)是在 k 为 5，3 和 1 时从加入噪声后的含水印图像中提取出的水印图像。可以看到，加入高达 0.5 的高斯噪声后图像已经非常模糊了，但提取出的水印图像依然很容易分辨，所以可以认为该算法对高斯噪声攻击具有很好的鲁棒性。

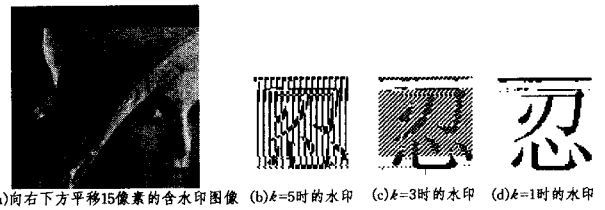


(a)加入0.5高斯噪声的含水印图像　(b)k=5时的水印　(c)k=3时的水印　(d)k=1时的水印

图 5　水印抗高斯噪声攻击的结果

3.4 平移攻击

图 6 是对含水印图像进行向下和向右各平移 15 个像素的平移攻击的实验结果。图 6(a)是进行平移后的含水印图像，图 6(b)－(d)是在 k 为 5，3 和 1 时从平移后的含水印图像中提取出的水印图像。结果表明，提取出的水印图像依然很容易分辨，所以可以认为该算法对平移攻击具有一定的鲁棒性。



(a)向右下方平移15像素的含水印图像　(b)k=5时的水印　(c)k=3时的水印　(d)k=1时的水印

图 6　水印抗平移攻击的结果

3.5 旋转攻击

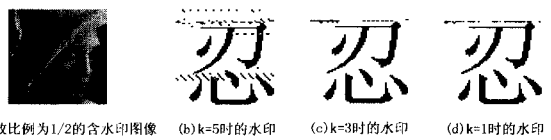
图 7 是对含水印图像进行 50°旋转攻击的实验结果。图 7(a)是进行旋转后的含水印图像，图 7(b)－(d)是在 k 为 5，3 和 1 时从旋转后的含水印图像中提取出的水印图像。即使图像旋转了 50°之多，提取出的水印图像依然容易分辨，所以可以认为算法对旋转攻击具有鲁棒性。

(a)旋转50°的含水印图像　(b)k=5时的水印　(c)k=3时的水印　(d)k=1时的水印

图 7　水印抗旋转攻击的结

3.6 缩放攻击

图 8 是对含水印图像进行比例为 1/2 的缩放攻击的实验结果（长和宽均缩小为原始大小的 1/2）。图 8(a)是进行缩放后的含水印图像，图 8(b)－(d)是在 k 为 5，3 和 1 时从缩放后的含水印图像中提取出的水印图像。结果表明，提取出的水印图像依然很容易分辨，所以可以认为该算法对缩放攻击具有鲁棒性。此外，水印的提取不需要像其他很多算法那样将缩放后的图像恢复成缩放前的原始大小，实现起来非常方便。



(a)缩放比例为1/2的含水印图像　(b)k=5时的水印　(c)k=3时的水印　(d)k=1时的水印

图 8　水印抗缩放攻击的结果

3.7 运算量比较

通过上述嵌入、提取实验以及抵抗各种攻击的实验，可以看到算法在水印的不可见性、嵌入容量以及鲁棒性上均具有较好的效果。仍然使用前面的 Lena 图像和二值水印图像，将提出的水印算法和文献[6]中的算法用 Matlab 进行仿真实验，试图对算法运算时间进行一个对比。对上面提到的所有的攻击，可以得到水印嵌入和提取算法平均耗费的运行时间。

从表 1 可知，文献[6]中的算法平均运行时间约为 0.29s，而我们提出的算法在 k 为 5，3 和 1 时，平均运行时间分别约为 310μs，590μs 和 1800μs。可以看到，随着 k 的减少，水印的鲁棒性越来越好，受攻击后提取出的水印效果越来越理想。同时，由于用来求不变质心的区域增多，算法耗时增加。但可以看到，即使在 k 为 1、计算量最大的情况下，平均时间也不到文献[6]中算法的平均时间的 1/100，显示出了良好的效率。

（下转第 298 页）

并发系统。二维抽象首先对所有进程单独进行抽象，然后利用参数化系统的设计思想，隐藏系统参数建立全系统的抽象模型，最大限度地剔除了原始系统中的冗余信息。TDA 模型关于 ACTL * 公式弱保持，而且在 TDA 模型中成立的单索引 ACTL * 公式，在任意规模的原始模型中也成立，为简化参数化系统验证提供了理论依据，也为相关研究工作奠定了良好的基础。

参 考 文 献

[1] 屈婉霞，李暾，郭阳，等. 谓词抽象技术研究[J]. 软件学报，2008，19(1)：27-38

[2] Shuvendu K L，Randal E B. Indexed Predicate Discovery for Unbounded System Verification[C]// Proc. of the 16th International Conference on Computer Aided Verification(CAV'04). Boston，USA：Springer，2004：276-289

[3] Amir P，Jessica Xu，Lenore Z. Liveness with(0；1；∞) Counter Abstraction[A]// Proc. of the 14th International Conference on Computer Aided Verification(CAV'02)[C]. Copenhagen，Denmark：Springer，2002：61-70

[4] Muralidhar T. Abstraction Techniques for Parameterized Verification[D]. Pittsburgh：Carnegie Mellon University，2006

[5] 曾红卫，缪淮扣. 构件组合的抽象精化验证[J]. 软件学报，2008，19(5)：1149-1159

[6] Konnov I V，Zakharov V A. An Invariant-Based Approach to the Verification of Asynchronous Parameterized Networks[C]// the 1st workshop on Invariant Generation(WING2007). Hagenberg，Austria：Springer，2007：41-55

[7] 屈婉霞，庞征斌，郭阳，等. 参数化系统二维抽象框架[J]. 国防科技大学学报，2010，32(1)：95-100

(上接第 281 页)

表 1 提出的水印算法和基于 Zernike 矩算法的运行时间(单位：ms)

	压缩	裁剪	加噪	平移	旋转	缩放
k=5	0.352	0.380	0.316	0.288	0.339	0.197
k=3	0.686	0.749	0.563	0.597	0.655	0.290
k=1	1.89	2.26	1.78	1.86	2.06	0.950
Zernike	297	360	302	282	348	153

结束语 本文首先研究了图像不变质心的特点和性质。为了使不变质心对几何攻击以及其他攻击具有更好的抵抗能力，对不变质心的提取方法进行了改进，不对整个图像求不变质心，而是对图像进行小波分解后，对小波低频域提取不变质心，取得了良好的效果。接着根据水印图像的大小自适应地对载体图像进行适当级的小波分解，将水印嵌入到对干扰不敏感的最后一级小波低频域，兼顾了水印的嵌入容量和不可见性。将含水印图像用改进的方法对小波域低频子图求得一系列基于不变质心的不变量后，基于这些不变量对攻击所具有的稳定性，定义了含水印图像的不变特征矩阵，并联合 Rijndael 加密技术实现了版权的认证，在提高水印算法可靠性的同时，使算法具有很好的鲁棒性。

该算法可嵌入实际的比特序列。实验结果表明，本文提供的水印算法能够抵抗包括平移、旋转、缩放等几何攻击在内的各种攻击，在提取水印时不需要原始载体图像和原始水印图像，从水印的透明性、水印嵌入容量和水印鲁棒性以及算法复杂度等指标来看，均具有较好的实效性。

参 考 文 献

[1] Lee C H，Lee H K，Suh Y G. Image Watermarking Resistant to Combined Geometric and Removal Attacks[J]. International Journal of Image and Graphics，2005，5(1)：37-66

[2] 金聪，彭嘉维. 基于图像投影序列的盲数字水印鲁棒检测方法[J]. 软件学报，2005，16(2)：295-302

[3] Lin P L，Hsieh C K，Huang P W. A Hierarchical Digital Watermarking Method for Image Tamper Detection and Recovery[J]. Pattern Recognition，2005，38(12)：2519-2529

[4] Kim H S，Lee H K. Invariant Image Watermark Using Zernike Moments[J]. IEEE Transactions on Circuits and Systems for Video Technology，2003，13(8)：766-775

[5] 李雷达，郭宝龙，刘雅宁. 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] 沃焱，韩国强. 基于修改的 Zernike 矩的抗几何攻击的数字水印方法[J]. 计算机科学，2009，36(5)：247-250，281

[7] Liu Jun，Yang Huijuan，Kot A C. Relationships and Unification of Binary Images Data-hiding Methods[C]// IEEE International Conference on Image Processing. 2005，1：I-981-4

[8] Ji Z，Jiang L，Jin J. An Improved Second Generation Digital Image Watermarking Scheme[C]// Mathematics of Data/Image Coding，Compression，and Encryption VI，with Applications. 2004，5208：218-223

[9] 凌贺飞，卢正鼎，邹复好. 抗几何攻击的数字水印技术综述[J]. 计算机工程与科学，2006，28(11)：42-47，50

[10] 钟桦，张小华，焦李成. 数字水印与图像认证——算法及应用[M]. 西安：西安电子科技大学出版社，2006

[11] Seo J S，Yoo C D. Image Watermarking Based on Invariant Regions of Scale-space Representation[J]. IEEE Transactions on Signal Process，2006，54(4)：1537-1549

[12] Jamil T. The Rijndael Algorithm[J]. IEEE Potentials，2004，23(2)：36-38

[13] 王炳锡. 数字水印技术[M]. 西安：西安电子科技大学出版社，2003

(上接第 294 页)

[5] Do M N，Vetterli M. The Contourlet transform：an efficient directional multiscale image representation [J]. IEEE Trans on Image Proc，2005，14(12)：2091-2106

[6] Zhou Jian-ping，Cunha A L，Do M N. Nonsubsampled contourlet transform：construction and application in enhancement[C] // Proceedings of International Conference on Image Processing (ICIP). Piscataway，NJ：IEEE，2005，1：469-472

[7] Cunha A L，Zhou Jian-ping，Do M N. The nonsubsampled contourlet transform：theory，design and applications [J]. IEEE Trans on Image Proc，2006，10(15)：3089-3101

[8] 罗子娟，吴一全. 基于 contourlet 变换的红外图像序列小目标检测技术[J]. 信号处理，2008，24(4)：676-679

[9] 吴一全，罗子娟，吴文怡. 基于 NSCT 的红外图像小目标检测技术[J]. 中国图象图形学报，2009，14(3)：477-481

[10] 唐志航，黄哲，张东衡，等. 基于尺度相关性的自适应图像增强新算法[J]. 计算机应用，2006，26(9)：2084-2086

[11] 韩敏，刘云侠. 改进的双小波空域相关混沌信号降噪方法[J]. 系统仿真学报，2009，21(15)：4743-4747

[12] 徐军，周翔，梁昌洪. 红外序列图像弱小目标检测算法[J]. 红外与激光工程，2003，32(4)：390-393

[13] 曾明，李建勋. 基于自适应形态学 Top-Hat 滤波器的红外弱小目标检测方法[J]. 上海交通大学学报，2006，40(1)：90-97