

## 一种抗缩放攻击的盲检测数字水印方案

周拥军, 尹忠海, 高大化

(空军工程大学 理学院, 西安 710051)

(chouyj008@163.com)

**摘要:**提出了一种抗缩放攻击的盲检测数字水印方案,在DCT域嵌入带有同步信息帧的水印信息,以及在空域构造具有固定间距、固定差分值的差分特征点网格是该方案的基本技术路线。给出了差分特征点网格的定义、嵌入和提取方法,提出了缩放系数的获取算法。实验结果表明,该数字水印系统对缩放攻击具有较好的鲁棒性。

**关键词:**数字水印;缩放攻击;差分特征点;网格;疑似网格点

**中图分类号:**TP309 **文献标志码:**A

### Blind digital watermarking scheme against scaling attack

ZHOU Yong-jun, YIN Zhong-hai, GAO Da-hua

(College of Science, Air Force Engineering University, Xi'an Shaanxi 710051, China)

**Abstract:** By embedding the watermarking with synchronous information frames in DCT domain and constructing a grid of difference feature points with fixed interval and fixed difference in space domain, a blind digital watermarking scheme against scaling attack was designed. The grid of difference feature points was defined, the embedding and extracting methods were given, and the algorithm for obtaining scaling factors was also presented. The experimental results show that the proposed scheme is robust to scaling attack.

**Key words:** digital watermarking; scaling attack; difference feature point; grid; suspicious grid point

## 0 引言

目前,鲁棒水印技术的研究取得了很大进展,但如何抵抗几何攻击仍然是水印领域所面临的重大困难<sup>[1-2]</sup>,成为当前数字水印产品商业化的障碍。抵抗几何攻击的数字水印的检测方法分为非盲检测和盲检测两种。非盲检测方法<sup>[3]</sup>在检测时需借助原始图像来计算几何变换因子,以实现水印检测的同步。盲检测水印方法大致分为三类<sup>[4]</sup>:1)几何不变量的方法;2)利用辅助信息的方法;3)基于特征的方法。本文以灰度图像为载体,设计了一种基于差分特征点网格、抗缩放攻击的盲检测数字水印方案。

## 1 抗缩放攻击的盲检测数字水印方案

本方案可以分为四个模块:数字水印的嵌入和提取模块、差分特征点网格的嵌入和提取模块。

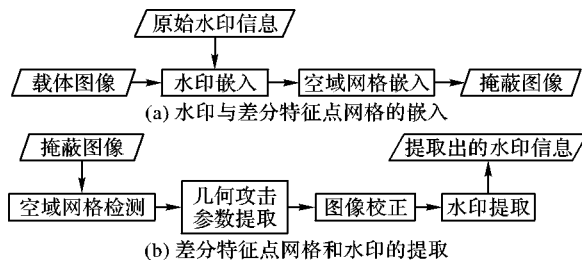


图1 基于差分特征点网格的数字水印嵌入与提取流程

数字水印的嵌入和提取部分参见文献[5],本文主要介绍差分特征点网格的嵌入和提取。

### 1.1 差分特征点网格的嵌入模块

为了获取掩蔽图像所遭受到的缩放攻击的相关系数,本文选择在空域上构造具有固定间距、固定差分值的差分特征点网格,然后根据遭受缩放攻击后网格的行(列)距变化来计算缩放系数。

#### 1.1.1 差分特征点

设 $I_{ij}$ 为灰度图 $I$ 在像素点 $(i, j)$ 处的灰度值, $M$ 为常整数,称满足:

$$|I_{i,j+1} - I_{i,j}| = |I_{i+1,j} - I_{i,j}| = M$$

的像素点 $(i, j)$ 为差分为 $M$ 的差分特征点。

为提高图像在受到缩放攻击时差分特征点检测的稳定性,单个差分特征点的实际构造方法<sup>[6]</sup>为:改变差分特征点周围的12个像素点的灰度值,使得右上的4个像素点和左下的4个像素点的灰度值相等,左上的4个像素点(包括特征点)的灰度值相等,而这两部分点的灰度值差分为 $M$ ,如图2所示。

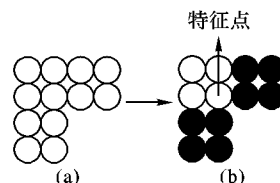


图2 单个差分特征点的构造

#### 1.1.2 网格的嵌入

在已经嵌有水印信息的图像中,以某像素点 $(i_0, j_0)$ 为起点,按照行距和列距均为 $D$ 的方式在图像中嵌入差分特征

收稿日期:2009-11-11;修回日期:2010-01-07。

基金项目:国家自然科学基金资助项目(60573040);陕西省自然科学基金资助项目(SJ08F10)。

作者简介:周拥军(1975-),男,四川蓬安人,讲师,硕士,主要研究方向:模式识别、图像处理;尹忠海(1964-),男,河北沧州人,副教授,博士,主要研究方向:计算机网络、信息安全;高大化(1979-),男,河南开封人,讲师,博士研究生,主要研究方向:信息安全、图像处理。

点,从而在整个图像中形成了一个矩形网格,如图3所示。其中, $D$ 为常整数,称为网格间距。

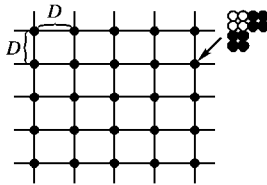


图3 差分特征点网格

差分特征点嵌入强度可以用两个指标描述,分别为差分值  $M$  和网格间距  $D$ 。由于在空域上嵌入差分特征点本质上是向载体图像添加噪声,去除攻击是对差分特征点的主要威胁,差分特征点添加后的透明性及鲁棒性是我们必须考虑的问题。通过大量实验,本文最终确定差分值  $M = 20$ , 网格间距  $D = 32$ 。

### 1.2 差分特征点网格的提取模块

提取网格时,根据差分特征点的嵌入方法,首先计算掩蔽图像各像素点的差分值,获取疑似网格点,然后通过将疑似网格点按行(列)投影,用试探法获取网格的行(列)距,从而计算出掩蔽图像所遭受的缩放攻击的系数。

#### 1.2.1 疑似网格点

掩蔽图像在受到攻击后,其差分特征点的差分值不会严格等于  $M$ , 因此在提取差分特征点时,引入了容差  $\delta$ , 称满足:

$$||I_{i,j+1} - I_{i,j}| - M| < \delta, ||I_{i+1,j} - I_{i,j}| - M| < \delta$$

的像素点  $(i,j)$  为疑似网格点。图4是从缩放到65%后的Lena图像中提取到的疑似网格点,可以看出有些点确为差分特征点,另一些点则为图像本身的纹理细节引起的噪声点。

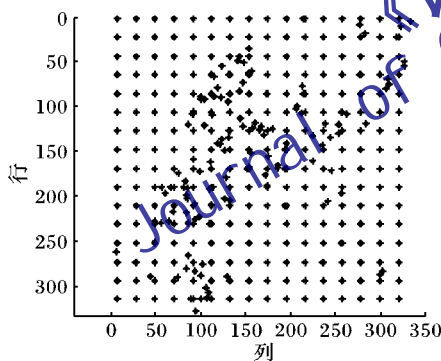


图4 疑似网格点

#### 1.2.2 缩放系数的获取算法

##### 1) 算法依据。

通过对实验数据和相关图形的分析,我们发现:

a) 同一行(列)的差分特征点在图像被缩放后,仍然位于同一行(列),也就是说嵌入在图像中的矩形网格在缩放后仍然是矩形网格。

b) 差分特征点在图像被缩放时丢失的可能性很小,而出现整行(列)的差分特征点丢失的概率几乎为0。

c) 虽然有噪声点的存在,但是差分特征点所在行(列)含有的疑似网格点数要远远大于其他行(列)的疑似网格点数,如图5所示。

d) 当因为缩放系数的缘故使得理论上的网格行(列)距不是整数时,实际的网格行(列)距并不相等,但它们彼此之间相差不超过1。例如,当网格间距  $D = 32$ , 同比缩放系数为108%时,理论上的网格行(列)距应为34.5,实际上的网

格行(列)距是按34、35、34、35、34、...的规律变化。

##### 2) 算法。

设灰度图像  $I$  在受到缩放攻击后,提取到的疑似网格点用一个0-1矩阵  $G$  表示,其中1代表疑似网格点,0代表非疑似网格点,  $G$  的行数(即图像  $I$  高度)为  $h$ , 列数(即图像  $I$  宽度)为  $w$ 。求  $I$  在宽度方向上的缩放系数  $Z_{col}$  的算法如下:

步骤1 按列投影。设  $L$  是一个长度为  $w$  的向量,令:

$$L(j) = \sum_{i=1}^h G(i, j); j = 0, 1, 2, \dots, w-1$$

步骤2 过滤。设  $Count$  为  $L$  中非0元素的个数,  $Sum$  为  $L$  中非0元素的和,  $avg = Sum/Count$ , 令:

$$M = \{i | L[i] \geq avg, i = 0, 1, \dots, w-1\}.$$

步骤3 试探法求列距  $D_{col}$ 。

1) 若  $M = \emptyset$ , 则转6); 否则, 令  $i_{first} = \min M, A = M \setminus \{i_{first}\}$ 。

2) 若  $A = \emptyset$ , 则转5); 否则, 令  $i_{second} = \min A, d = i_{second} - i_{first}, n = 1$ 。

3) 若  $|w - i_{first}| < 3d$ , 则转5); 若  $d \leq 4$ , 则令  $A = A \setminus \{i_{second}\}$ , 转2); 否则, 令  $i_{now} = i_{second}, i_{next} = i_{now} + d$ 。

4) 若  $i_{next} \geq w$ , 则转7); 若  $i_{next} = 4$ , 则令  $n = n + 1, i_{now} = i_{next}, i_{next} = i_{now} + d$ , 转4); 若  $(i_{next} - 1) \in A$ , 则令  $n = n + 1, i_{now} = i_{next} - 1, i_{next} = i_{now} + d$ , 转4); 若  $(i_{next} + 1) \in A$ , 则令  $n = n + 1, i_{now} = i_{next} + 1, i_{next} = i_{now} + d$ , 转4); 否则, 令  $A = A \setminus \{i_{second}\}$ , 转2)。

5) 令  $M = M \setminus \{i_{first}\}$ , 转1)。

6) 令  $D_{col} = 0$ , 停止。

7) 令  $D_{col} = (i_{now} - i_{first})/n$ , 停止。

步骤4 计算  $I$  在宽度方向上的缩放系数  $Z_{col}$ 。

$$Z_{col} = D_{col}/D$$

其中  $D$  为网格间距。

类似地, 可求  $I$  在高度方向上的缩放系数  $Z_{row}$ 。

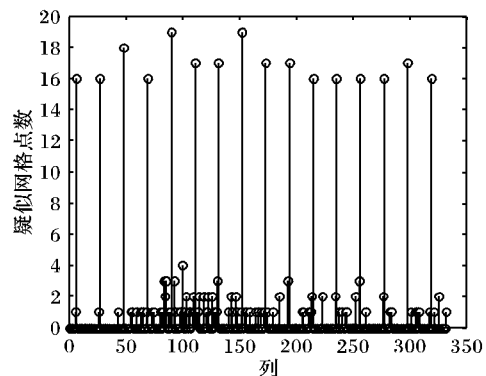


图5 疑似网格点在列方向上的统计图

## 2 实验结果与分析

本数字水印系统搭建在一个PC上, 开发软件为VC++ 6.0。实验中选用尺寸为  $512 \times 512$  的Lena图像, 水印是一个有意义的二值图像, 如图6所示。

为验证算法对缩放攻击的校正性能, 参照文献[7]进行了相应的缩放攻击实验, 并将本文算法计算得到的缩放系数与文献[7]的进行对比, 见表1。

本文算法不但可以抗对称缩放(即比例缩放)攻击, 而且可以抵抗非对称缩放攻击。表2是Lena图像进行非对称缩放攻击的实验结果, 表中  $Z_x$ 、 $Z_y$  分别表示Lena图像在宽度和

高度方向上的缩放系数。

表1 与文献[7]的实验结果对比

(对称) 缩放攻击系数	本文算法结果	文献[7]算法结果
0.5	0.5000	0.4943
0.7	0.7000	0.7045
0.9	0.9000	0.8978
1.0	1.0000	1.0000
1.1	1.1000	1.0993
1.3	1.3013	1.2998
1.5	1.5000	1.4898



(a) 载体图像

NowT  
2010  
0101

(b) 水印图像

图6 载体图像和水印图像

表2 对Lena图像实施非对称缩放攻击的实验结果

缩放攻击系数	网格分析得到的系数	水印提取结果
$Z_x = 0.80$	$Z_x = 0.8013$	NowT
$Z_y = 0.85$	$Z_y = 0.8498$	2010
		0101
$Z_x = 1.03$	$Z_x = 1.0292$	NowT
$Z_y = 1.16$	$Z_y = 1.1604$	2010
		0101
$Z_x = 1.46$	$Z_x = 1.4604$	NowT
$Z_y = 1.50$	$Z_y = 1.5000$	2010
		0101
$Z_x = 2.06$	$Z_x = 2.0604$	NowT
$Z_y = 1.98$	$Z_y = 1.9813$	2010
		0101
$Z_x = 1.04$	$Z_x = 1.0402$	NowT
$Z_y = 1.91$	$Z_y = 1.9104$	2010
		0101

(上接第1232页)

变,降低了管理的复杂度。针对权限继承中可能出现的两种冲突,根据不同的需求采取不同的策略加以解决。对增大权限传播深度是否违背静态职责分离约束,给出了一个高效的检测算法。该算法保证在执行的操作不违背静态职责分离约束的前提下,才执行相应的操作,保证了系统的安全性。

#### 参考文献:

- [1] SANDHU R S, COYNE E J, FEINSTEIN H L, *et al.* Role-based access control models [J]. IEEE Computer, 1996, 29(2): 38 - 47.
- [2] FERRAILOLO D F, SANDHU R, GAVRILA S, *et al.* Proposed NIST standard for role-based access control [J]. ACM Transactions on Information and System Security, 2001, 4(3): 224 - 274.
- [3] ANSI/INCITS 359-2004, Information technology-role based access control [S]. International Committee for Information Technology Standards, 2004.
- [4] 钟华,冯玉琳,姜洪安. 扩充角色层次关系模型及其应用[J]. 软件学报, 2000, 11(6): 779 - 784.

#### 实验结果分析:

1) 本文算法计算得到缩放攻击的系数,其精度是比较高的,而且当实验图像尺寸增大时,由于嵌入的差分特征点数量增加,精度也随之增大。例如,采用  $512 \times 512$  的Lena图像进行实验时,精度保持在  $10^{-3}$  这个数量级;采用  $2048 \times 2048$  的世界地图进行实验时,精度就提升到  $10^{-4}$  这个数量级。

2) 采用本文算法计算得到的缩放攻击系数的精度,足以帮助水印提取模块完成图像校正,顺利提取水印。

### 3 结语

本文提出了一种基于差分特征点、抗缩放攻击的盲检测数字水印方案。该方案中获取缩放系数的算法具有简单、速度快、精度高等特点,但也必须看到该算法局限于缩放攻击,不适用于旋转攻击和扭曲攻击。下一步将在此基础上研究如何让数字水印系统能够抵抗旋转攻击和扭曲攻击,更进一步的,研究如何在不知道攻击类型的情况下顺利地提取水印。

#### 参考文献:

- [1] PETITCOLAS F A P, ANDERSON R J, KUBN M G. Attacks on copyright marking system[C]// Proceedings of the 2nd International Workshop on Information Hiding, LNCS 523. Berlin: Springer-Verlag, 1998: 218 - 238.
- [2] LU ZHENGMING, XING WEN, XU DIANGUO, *et al.* Digital image watermarking technique base on vector quantization with labeled codewords[J]. IEEE Transaction on Information and System, 2003, E86-D(12): 2786 - 2789.
- [3] 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[J]. 浙江大学学报:工学版, 2003, 37(4): 386 - 392.
- [4] 刘九芬,王振武,黄达人. 图像水印抗几何攻击研究综述[J]. 电子与信息学报, 2004, 26(9): 1495 - 1503.
- [5] 周翔翔,尹忠海,王欣,等. 基于结构化编码的抗剪切图像数字水印[J]. 计算机应用, 2009, 29(5): 1324 - 1326.
- [6] 尹忠海,周拥军,高大化,等. 基于差分特征点网格的数字水印抗缩放性能[J]. 空军工程大学学报:自然科学版, 2009, 10(4): 76 - 80.
- [7] 张晓黎. 一种抗几何失真的水印校正方法研究[J]. 计算机应用与软件, 2009, 26(7): 14 - 16.

- [5] 邵佳伟,余本功,杨善林. 一种针对信息网格RBAC模型私有权限问题的有效解决方案[J]. 计算机应用研究, 2007, 24(4): 133 - 135.
- [6] 刘建圻,曾碧,郑秀璋. 基于RBAC权限管理模型的改进与应用[J]. 计算机应用, 2008, 28(9): 2449 - 2451.
- [7] 张世龙,沈玉利. RBAC模型中角色继承关系的研究与改进[J]. 计算机应用研究, 2009, 26(6): 2362 - 2364.
- [8] LI NINGHUI, BIZRI Z, TRIPUNITARA M V. On mutually-exclusive roles and separation of duty [C]// Proceedings of the 11th ACM Conference on Computer and Communications Security. New York: ACM Press, 2004: 42 - 51.
- [9] CHEN HONG, LI NINGHUI. Constraint generation for separation of duty [C]// Proceedings of the 11th ACM Symposium on Access Control Models and Technologies. New York: ACM Press, 2006: 130 - 138.
- [10] LI NINGHUI, TRIPUNITARA M V, BIZRI Z. On mutually exclusive roles and separation-of-duty [J]. ACM Transactions on Information and System Security, 2007, 10(2): 5.