

基于差分网格的抗 RSD 攻击盲指纹方案

赵伟光,尹忠海,周拥军,梁 爽

(空军工程大学 理学院,西安 710051)

(zwgl111@yahoo.com.cn)

摘 要:为了提高数字指纹的抗综合攻击能力,构造了抗旋转、缩放、扭曲攻击(简记为 RSD 攻击)的数字指纹嵌入和提取策略。设计了数字指纹的空域—DCT 域联合嵌入方案,给出了差分特征点的构造方法,以及基于差分特征点网格的数字指纹嵌入与提取算法,设计了高精度攻击参数辨识算法。实验结果表明,所提方案攻击参数辨识精度达到亚像素级,能抵抗缩放系数大于 0.5 的缩放攻击,45°角以内的任意旋转攻击,以及 25°角以内的任意扭曲攻击;且指纹提取效果并不因旋转角度的增大而降低,也不因扭曲角度的增大而有明显降低。该方案提高了数字指纹的鲁棒性,使数字指纹系统在能抵抗去除攻击、剪切、平移、粘贴攻击(简称 CTP 攻击)的同时具备抵抗 RSD 攻击的能力。

关键词:RSD 攻击;差分网格;数字指纹;盲指纹

中图分类号:TP309.2 **文献标志码:**A

Blind fingerprint scheme against RSD attacks based on differential grid

ZHAO Wei-guang, YIN Zhong-hai, ZHOU Yong-jun, LIANG Shuang

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

Abstract: The construction of digital fingerprint embedding and acquisition scheme for anti-rotation, anti-scaling and anti-distortion attack can improve the anti-attack capability of the digital fingerprint. The designed spatial-DCT (Discrete Cosine Transform) domain combinational embedding scheme of digital fingerprint provided the construction of differential characteristic point, on which the digital fingerprint embedding and acquisition algorithm was proposed. And an attack parameter recognition algorithm with high accuracy was presented. The simulation results show that the accuracy of attack recognition algorithm can be the order of sub-pixel and can resist the scaling attack with parameter larger than 0.5, any rotation attack with angle less than 45° and any distortion attack with angle less than 25°. In addition, the effect of the proposed scheme would not decrease with the increase of the rotation and distortion angle. The proposed scheme improves the robustness of the digital fingerprint and enables the digital fingerprint system to resist the removal and CTP (cutting, trimming, pasting) attack as well as RSD (rotation, scaling, distortion) attack.

Key words: RSD (Rotation, Scaling, Distortion) attack; differential grid; digital fingerprint; blind fingerprint

0 引言

数字指纹技术通过向数字作品中嵌入最终用户 ID 信息,以确保能够进行泄密追踪。因此,必须要研究抵抗各类攻击的算法以增强数字指纹的稳健性能。

数字指纹技术发展到今天,已有了大量不同的算法,但是很多数字指纹算法只能对抗一般的信号处理,不能抵抗甚至很微小的几何攻击^[1-2]。抗几何攻击数字指纹的检测方法可分为非盲检测和盲检测两种。非盲检测方法^[3]在检测时需借助原始图像来计算几何变换因子,以实现指纹检测的同步。盲检测指纹方法大致分为三类^[4]:几何不变量的方法^[5-10]、利用辅助信息的方法^[11-13]和基于特征的方法^[14-16]。

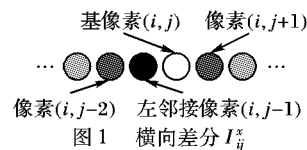
旋转(Rotation)、缩放(Scaling)和扭曲(Distortion)攻击统称为 RSD 攻击,其破坏方式是一致的,所产生的后果都是使得掩蔽图像的上、下或左、右侧的数据成片丢失或失效。

本文以数字正射影像为载体,设计一种基于差分特征点网格的抗 RSD 攻击盲检测数字指纹方案,使数字指纹系统在能抵抗去除攻击、CTP(剪切(cutting)、平移(trimming)、粘贴(pasting))攻击的同时具备抵抗 RSD 攻击的能力。

1 差分网格

1.1 差分特征点

定义 1 横向差分。设 I_{ij} 为灰度图 I 像素点 (i, j) 的灰度值,其中 i, j 分别为该像素点的横纵坐标,该像素点称为基像素。称该像素点灰度值 I_{ij} 和其左侧相邻像素点灰度值 $I_{i, j-1}$ 之差的绝对值 $|I_{ij} - I_{i, j-1}|$ 为该像素点的横向差分,记为 I_{ij}^x ,如图 1 所示。根据 CTP 攻击的特性,以遥感影像为载体,通过对指纹进行帧编码,使得指纹信息和同步字段绑定在一起,采用基于图像分片的多版本嵌入及图像有效分片定位的提取策略,设计相应的抗 CTP 攻击 DCT 域嵌入及提取方案。分片嵌入策略如图 1 所示。



定义 2 纵向差分。设 I_{ij} 为灰度图 I 像素点 (i, j) 的灰度值,其中 i, j 分别为该像素的横纵坐标,该像素点称为基像素。

收稿日期:2011-01-30;修回日期:2011-06-22。

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:赵伟光(1956-),男,河北安国人,副教授,主要研究方向:图像处理、信息安全;尹忠海(1964-),男,河北沧州人,教授,博士,主要研究方向:信息隐藏、移动自组织网络。

素。称该像素点灰度值 I_{ij} 和其上方相邻像素点灰度值 $I_{i,j-1}$ 之差的绝对值 $|I_{ij} - I_{i,j-1}|$ 为该像素点的纵向差分, 记为 I_{ij}^y , 如图2所示。

定义3 差分特征点。设 I_{ij} 为灰度图 I 像素点 (i, j) 的灰度值, 其中 i, j 分别为该像素的横纵坐标。若像素 (i, j) 的横向差分值和纵向差分值都为固定值 M , 即 $I_{ij}^x = I_{ij}^y = M$, 则称该像素点为差分值为 M 的差分特征点, 如图3所示。

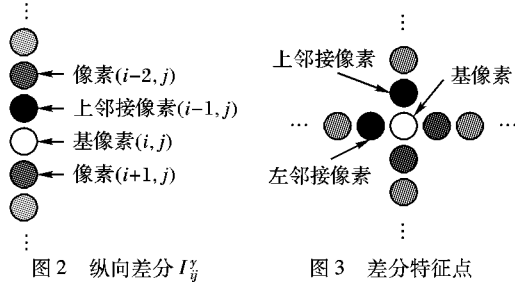
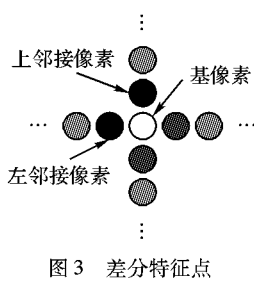
图2 纵向差分 I_{ij}^y 

图3 差分特征点

1.2 单个差分特征点的构造算法

算法的基本思想是调整特征点附近12个像素点的值, 如图4所示, 使得差分特征点右上的4个像素点和左下的4个像素点的值都相等, 左上的4个像素点的值相等, 这两部分点的灰度值差值为 M , 即图4中白色部分4个像素点和黑色部分8个像素点的差值为固定值 M , 像素点 (i, j) 为差分特征点。

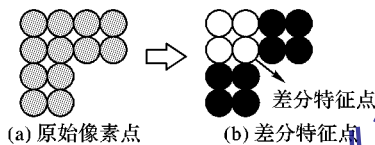


图4 单个差分特征点的构造

由于空域嵌入的差分特征点其本质仍然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。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 , 其中 D 如图5所示。两个嵌入强度参数中 D 对嵌入透明性的影响最大, 是影响嵌入透明性的主要因素, 不能太小。差分值 M 主要影响差分特征点的鲁棒性: 如果 M 过大, 载体图像与掩蔽图像的相似度及信噪比不能满足要求, 甚至连视觉透明性都无法满足; 如果 M 过小, 去除攻击将会去掉某些差分特征点, 影响网格提取精度。本文实验表明, 若差分值 M 大于25, 视觉透明性无法满足; 若差分值 M 小于17, 网格提取精度降低, 故取差分值 $M = 20$ 。若取网格间距为 $D = 32$, 差分值 $M = 20$, 图像相似度 Sim_2 满足大于0.98的要求, 信噪比约为41.6 dB, 不符合要求; 取网格间距为 $D = 48$, 差分值 $M = 20$, 图像相似度 Sim_2 满足大于0.98的要求, 信噪比大于43 dB。故项目最终确定网格间距为 $D = 48$, 差分值 $M = 20$ 。

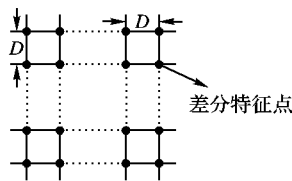


图5 差分特征点网格

算法1 差分特征点构造算法。

步骤1 设像素 (i, j) 为待构造的差分特征点, 取差分值为 $M = 20$, 取像素点 (i, j) 附近四行的12个像素点。其中第

$i+1$ 行和第 i 行各四个像素点, 第 $i-1$ 行和第 $i-2$ 行各两个像素点, 如图4(b)所示。

第 $i+1$ 行: $(i+1, j-2), (i+1, j-1), (i+1, j), (i+1, j+1)$;

第 i 行: $(i, j-2), (i, j-1), (i, j), (i, j+1)$;

第 $i-1$ 行: $(i-1, j), (i-1, j+1)$;

第 $i-2$ 行: $(i-2, j), (i-2, j+1)$ 。

步骤2 提取这12个像素点的值, 分别记为:

第 $i+1$ 行: $I_{i+1, j-2}, I_{i+1, j-1}, I_{i+1, j}, I_{i+1, j+1}$;

第 i 行: $I_{i, j-2}, I_{i, j-1}, I_{i, j}, I_{i, j+1}$;

第 $i-1$ 行: $I_{i-1, j}, I_{i-1, j+1}$;

第 $i-2$ 行: $I_{i-2, j}, I_{i-2, j+1}$ 。

计算这12个像素点的像素平均值 $\text{mid}(I_{ij})$ 。

步骤3 调整 $I_{ij}, I_{i,j-1}, I_{i-1,j}$ 三个像素点的值, 使得像素点 (i, j) 的横向差分值和纵向差分值都为 $M = 20$ 。为此, 令:

$$I_{ij} = \text{mid}(I_{ij}) - M/2 = \text{mid}(I_{ij}) - 10$$

$$I_{i, j-1} = \text{mid}(I_{ij}) + M/2 = \text{mid}(I_{ij}) + 10$$

$$I_{i-1, j} = \text{mid}(I_{ij}) + M/2 = \text{mid}(I_{ij}) + 10$$

步骤4 为使 $I_{ij}^x = I_{ij}^y = M$ 且具有较强的稳定性, 根据调整后的 $(i, j), (i, j-1), (i-1, j)$ 三个像素点的值, 调整其他9个像素点的灰度值。

1.3 差分特征点网格的嵌入

设载体图像高为 M , 宽为 N , 令 $m = \lfloor M/D \rfloor, n = \lfloor N/D \rfloor$, 其中 $D = 48$, 则载体图像应当嵌入的特征点数为 $m \times n$, 应嵌入特征点的像素点坐标为:

$$(i, j) = (k \times D, l \times D); 1 \leq k \leq m, 1 \leq l \leq n$$

在已经嵌有指纹信息的图像中, 以像素点 $(0, 0)$ 为起点, 调整图像中相应点附近的12个像素点的值, 构成一个差分特征点, 且相邻差分特征点之间的距离为固定值 D 。在整个图像中最终确定了一个矩形网格, 单个网格是大小为 $D \times D$ 的正方形, 如图5所示。大量实验表明: 选择 D 的大小为48像素可保证特征点具有较好的不可见性, 此时称如图5所示的网格为差分特征点网格, 相应差分特征点在本文后续内容中统称为网格节点, 网格节点嵌入算法见算法2。

算法2 网格节点嵌入算法。

步骤1 设载体图像高为 M , 宽为 N , 令 $m = \lfloor M/D \rfloor, n = \lfloor N/D \rfloor$, 其中 $D = 48$ 。

步骤2

For $k = 1$ to m

For $l = 1$ to n

调用算法1在像素点 $(k \times D, l \times D)$ 嵌入差分特征点

Next l

Next k

2 差分网格的抗 RSD 攻击盲指纹方案

基于差分特征点网格的数字指纹方案首先要提取时域上嵌入的网格节点, 根据正方形网格经历 RSD 攻击后的特性, 判断 RSD 攻击类型并计算参数, 并根据攻击类型及参数校正图像。在频域上通过寻找同步信息帧方法进行图像有效分片定位, 获得指纹所在的位置, 最后进行指纹提取。

2.1 疑似网格点的提取

提取时首先计算各像素点的差分, 若像素点 (i, j) 满

足

$$|I_{ij}^x - M| < \delta, \quad |I_{ij}^y - M| < \delta$$

即认为像素点 (i, j) 为网格节点。由于存在攻击或噪声, 这些点只能是疑似网格点, 对 Lena 图像进行差分特征点嵌入并缩放后的疑似网格点如图 6 所示。其中图 (a) 中的横坐标、纵坐标分别为载体图像的横坐标、纵坐标; 图 (b) 中的横坐标为载体图像的横坐标, 单位是像素; 纵坐标为疑似网格点按列统计的数量。在图 6 中, 有些点的确是嵌入的网格节点, 另一些点则是原始图像的纹理细节形成的 (差分值恰约等于 M)。为此给出以下定义。

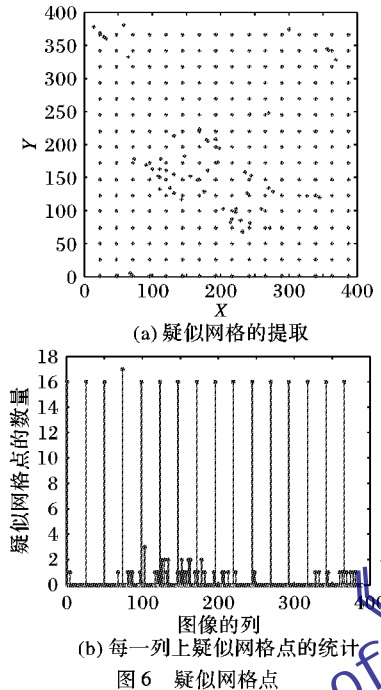


图 6 疑似网格点

定义 4 设 I 为掩蔽图像, 若像素点 (i, j) 满足: $|P_x(i, j) - M| < \delta, |P_y(i, j) - M| < \delta$, 则称像素点 (i, j) 为疑似网格点。

如图 6 所示为 512×512 的 Lena 图缩放为原来的 76% 后提取的疑似网格点, 从图中可以看出有一些噪声点。

2.2 RSD 攻击参数估计

在 RSD 攻击下, 载体图像中的网格必然发生变形。在缩放攻击下, 载体图像中的网格构成长方形; 在旋转攻击下, 载体图像中的网格仍构成边长为 D 的正方形; 在扭曲攻击下, 载体图像中的网格构成平行四边形。即使同时进行 RSD 攻击, 载体图像中的网格也构成平行四边形, 如图 7 所示。

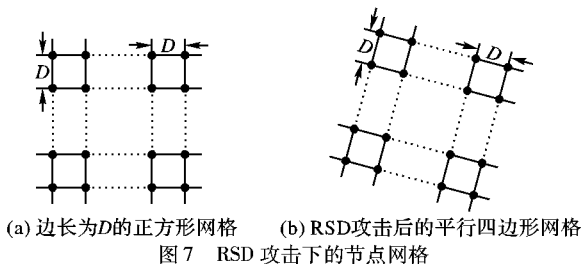


图 7 RSD 攻击下的节点网格

RSD 攻击严重破坏了掩蔽图像的同步信息, 使得嵌于变换域的指纹信息无法提取, 但指纹信息并未遭受大的破坏, 仍然存在于某一特定像素区域, 我们的任务就是要想办法识别攻击参数, 恢复掩蔽图像的同步信息并提取指纹。

RSD 攻击后载体图像中的网格构成平行四边形, 一般描述平行四边形的参数有四个, 分别为两条边长和两个夹角, 如图 8 所示。两个夹角可以有多种形式, 典型的是图中所给的两边夹角型参数和边与 X 轴夹角型参数, 为便于后续攻击参数辨识算法设计, 选择图 8(b) 所示的边与 X 轴夹角型参数。

考虑到 RSD 攻击后节点网格为平行四边形, 设计了如算法 3 所示的网格提取算法, 其核心思想就是要在所有疑似网格节点中找出正确的平行四边形。

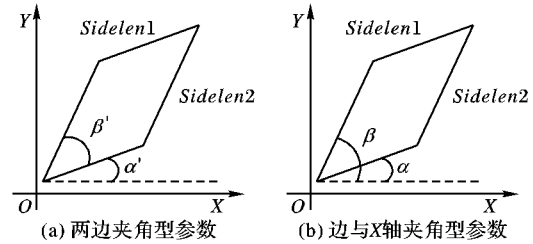


图 8 网格平行四边形参数

算法 3 RSD 攻击的参数估计算法。

步骤 1 设掩蔽图像为 I , 计算 I 的各像素点差分, 求出疑似网格点, 设所有疑似网格点的集合为 S , 令 $T = \emptyset$ 。

步骤 2 取最靠近图像中心的疑似网格点 x_c , 令 $x_0 = x_c$ 。

步骤 3 x_0 附近疑似网格点构成的平行四边形分析。

1) 以 x_0 为种子点, 求出距 x_0 最近的 n (实际项目取为 30) 个疑似网格点, 构成集合 R , 设 $R = \{x_1, x_2, \dots, x_n\}$;

2) 求出 R 中所有与 x_0 不构成三点共线的点对 $x_{11}x_{21}, \dots, x_{1m}x_{2m}$, 令 $k = 1$;

3) 取点对 $x_{1k}x_{2k}$, 以 x_{1k}, x_{2k} 为两个候选点, 计算 x_0, x_{1k}, x_{2k} 的 13 个边对称点记为 y_1, y_2, \dots, y_{13} ;

4) 若存在 $u \in S$, 使得 $\|u - y_i\|_\infty \leq 2$, 即认为 $y_i \in S$, 计算 13 个边对称点 y_1, y_2, \dots, y_{13} 中属于 S 的点的个数, 若大于 9, 则可以认定 x_0, x_{1k}, x_{2k} 为由网格点构成的平行四边形的三个顶点, 转 4);

5) 令 $k = k + 1$, 若 $k < m$, 转 3);

若 $k \geq m$, 取 $T = T \cup \{x_0\}$, 令 $S = S - T$, 取 S 中与 x_c 距离最近的点作为新的 x_0 , 转 3)。

步骤 4 计算输出平行四边形的边与 X 轴的两个夹角 α 、 β , 平行四边形的两个边长 $Sidelen1$ 和 $Sidelen2$, 结束。

采用算法 3 进行 RSD 攻击的参数估计的实验结果如图 9 所示, 图中掩蔽图像沿逆时针进行了 30° 旋转。

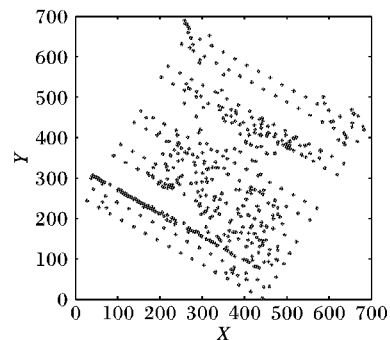


图 9 算法提取出的旋转后网格

算法输出的四个参数分别为 $Sidelen1/D = 0.9587$ 和 $Sidelen2/D = 1.0391$, $\alpha = 61.9235$, $\beta = 151.0241$ 。虽然未对图像进行任何缩放操作, 但检出的缩放比例分别为 $Sidelen1/D = 0.9587$ 和 $Sidelen2/D = 1.0391$, 缩放比例误差

分别为0.0422和0.0391。对于256×256的Lena图像,恢复后总的纵横误差分别为10个像素,无法恢复DCT嵌入的同步信息,指纹提取失败。

2.3 图像的同步信息恢复与指纹提取

基于差分特征点网格的数字指纹方案在指纹信息提取前必须首先根据1.2节、1.3节和2.2节算法提取出的攻击参数进行图像恢复。

若掩蔽图像只受到缩放攻击,则网格节点四边形为边平行于坐标轴的矩形,缩放系数分别为 $Sidelen1/D$ 和 $Sidelen2/D$ 。因此若提取出的网格节点四边形为边平行于坐标轴的矩形,可等效地认为只受到了缩放攻击,此时恢复同步信息必需的两个参数为 $Sidelen1$ 和 $Sidelen2$ 。

若掩蔽图像只受到旋转攻击,则网格节点四边形为正方形, $Sidelen1 = D$ 且 $Sidelen2 = D$ 。因此若提取出的网格节点四边形为正方形(边不平行于坐标轴,否则认为不存在攻击),可等效地认为只受到了旋转攻击,此时恢复同步信息必需的一个参数为 α 或 β 。

若掩蔽图像只受到沿一个坐标轴的扭曲攻击,则网格节点四边形为一条边平行于坐标轴的平行四边形。因此若提取出的网格节点四边形为一条边平行于坐标轴的平行四边形,可等效地认为只受到了扭曲攻击,此时恢复同步信息必需的一个参数为 α 或 β 。

对于有多种不同RSD形式的综合攻击,网格节点必然构成平行四边形。本章提出的参数估计提取算法能有效辨识攻击参数,精度很高,但数字指纹的提取效果很差,初步判定与本文采用的图像恢复算法有关。目前我们正试图从理论上确定攻击参数辨识效果好但指纹提取效果差的原因,以期解决综合形式的RSD攻击问题。

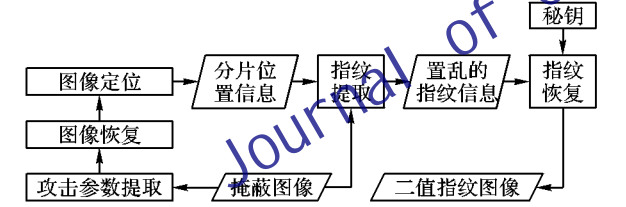


图 10 基于差分特点的指纹提取方案

3 仿真结果

采用如图1基于差分特征点网格的指纹提取方案,掩蔽图像为2048×2048大小的灰度图,提取时不指定RSD攻击类型,由程序自行判断并进行攻击参数辨识、图像恢复、指纹提取。

实验结果表明该系统掩蔽图像具有很好的视觉透明性,按 Sim_2 计算的图像相似度均在0.99以上。方案也具有较好的鲁棒性,指纹提取效果好,能够有效地抗多数去除攻击、CTP攻击和RSD攻击。本文以下仅给出RSD攻击实验结果。

3.1 缩放测试

缩放攻击可同时进行纵向和横向缩放,攻击由Photoshop CS3实施。缩放攻击参数、算法得到的缩放因子、指纹提取结果见表1,提取指纹相似度见表2。

3.2 旋转测试

旋转攻击可进行45°角以内的任意旋转,攻击由Photoshop CS3实施。旋转攻击参数、算法得到的旋转参数(单位:°)、指纹提取结果见表3、4。

3.3 扭曲测试

扭曲攻击(也称几何形变)由Windows自带的画图工具实施,顺时针为正方向,可进行25°角以内的任意扭曲,为便于软件实现,假设顺时针为正方向。扭曲攻击参数、算法得到的扭曲攻击参数、指纹提取结果见表5、6。

表 1 缩放攻击测试结果

缩放攻击参数		算法提取出的缩放因子		指纹提取结果
横向比例	纵向比例	横向比例	纵向比例	
1.10	1.10	1.0999	1.1000	图11(a)
1.20	1.20	1.2002	1.2004	图11(b)
1.40	1.40	1.4001	1.4000	图11(c)
1.70	1.70	1.7002	1.7004	图11(d)
0.95	0.95	0.9498	0.9500	图11(e)
0.90	0.90	0.9001	0.9000	图11(f)
0.80	0.80	0.7998	0.7996	图11(g)
0.70	0.70	0.7002	0.7004	图11(h)
0.50	0.50	0.5000	0.5000	图11(i)
0.80	1.10	0.7996	1.1002	图11(j)
0.90	1.00	0.8998	1.0000	图11(k)
1.20	0.90	1.2004	0.8998	图11(l)
1.00	1.20	1.0000	1.2004	图11(m)

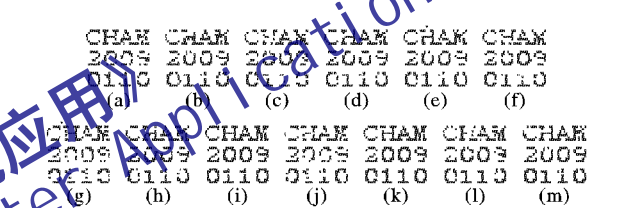


图 11 缩放攻击测试提取结果

表 2 抗缩放攻击提取指纹相似度

序号	相似度 Sim_5	相似度 Sim_4
1	0.7628	0.9141
2	0.7601	0.9121
3	0.7348	0.8926
4	0.7655	0.9160
5	0.7710	0.9199
6	0.7738	0.9219
7	0.7184	0.8789
8	0.7497	0.9043
9	0.9381	0.9941
10	0.7207	0.8809
11	0.9054	0.9863
12	0.7655	0.9160
13	0.8248	0.9531

表 3 旋转攻击测试结果

旋转攻击参数	算法得到的旋转参数/(°)	指纹提取结果
顺时针 旋转/(°)	8	图12(a)
	12	图12(b)
	16	图12(c)
	24	图12(d)
	32	图12(e)
逆时针 旋转/(°)	6	图12(f)
	10	图12(g)
	20	图12(h)
	30	图12(i)
	40	图12(j)

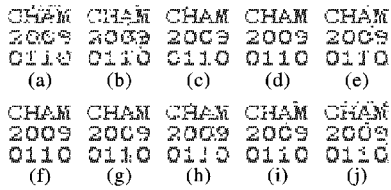


图12 旋转攻击测试提取结果

表4 抗旋转攻击提取指纹相似度

序号	相似度 Sim_5	相似度 Sim_4
1	0.6842	0.8477
2	0.7300	0.8887
3	0.8814	0.9785
4	0.9124	0.9883
5	0.8142	0.9473
6	0.9285	0.9922
7	0.8526	0.9668
8	0.7601	0.9121
9	0.8711	0.9746
10	0.7655	0.9160

表5 扭曲攻击测试结果(参数精度保留小数点后6位)

扭曲攻击参数	算法得到的扭曲参数/(°)	指纹提取结果
水平 扭曲/(°)	-4	图13(a)
	-7	图13(b)
	10	图13(c)
	18	图13(d)
	30	图13(e)
垂直 扭曲/(°)	6	图13(f)
	-9	图13(g)
	14	图13(h)
	-16	图13(i)
	-24	图13(j)

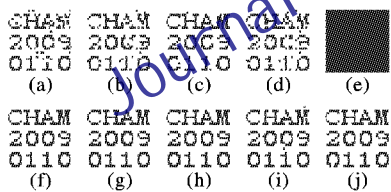


图13 扭曲攻击测试提取结果

表6 抗扭曲攻击提取指纹相似度

序号	相似度 Sim_5	相似度 Sim_4
1	0.7471	0.9023
2	0.7628	0.9141
3	0.8526	0.9668
4	0.7300	0.8887
5	0.0418	-0.4023
6	1.0000	1.0000
7	1.0000	1.0000
8	1.0000	1.0000
9	0.9381	0.9941
10	0.9494	0.9961

通过对提取效果的分析可以看出,系统具有较好的鲁棒性,能够有效地抵抗非综合的RSD攻击。主要体现如下:

1) 缩放攻击可同时进行纵向和横向缩放,能抵抗缩放系数大于0.5的缩放攻击,甚至在缩放系数等于0.5时仍有很

好的提取效果。

2) 旋转攻击可进行45°以内的任意旋转,指纹提取效果并不因旋转角度的增大而降低,如旋转40°时的指纹提取效果甚至优于旋转12°时的提取效果。事实上本文所提出的方案可抵抗任意角度的旋转攻击,只是在旋转攻击角度大于45°时程序辨识出的旋转角度存在两种可能。由于泄密者通常只进行小角度旋转,故软件规定旋转角度小于45°。

3) 扭曲攻击可进行25°以内的任意扭曲,指纹提取效果并不因扭曲角度的增大而有明显降低。

4 结语

本文提出了一种基于差分特征点网格的抗RSD攻击数字指纹,该方案是一种数字图像盲指纹方案,对RSD攻击具有很好的鲁棒性,且能够有效地抵抗多数常规攻击和CTP攻击。本文所提方法既不需要原始载体图像,也不需要数字水印信息,实现了完全盲检测,由仿真结果可知检测效果良好。

参考文献:

- [1] PETITCOLAS F A P, ANDERSON R J, KUHN M G. Attacks on copyright marking system [C]// Proceedings of the 2nd International Workshop on Information Hiding, LNCS-1525. London, UK: Springer-Verlag, 1998: 218-238.
- [2] LU ZHENGMING, XING WEN, XU DIANGUO, et al. Digital image watermarking technique based on vector quantization with labeled codewords [J]. IEICE Transactions on Information and System, 2003, E86-D(12): 2786-2789.
- [3] 刘九芬,王振武. 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,黄达人,黄继武. 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] LIN C Y, WU M, BLOOM J A, et al. Rotation, scale, and translation resilient watermarking for images [J]. IEEE Transactions on Image Processing, 2001, 10(5): 767-782.
- [6] LICKS V, JORDAN R. On digital image watermarking robust to geometric transformations [C]// 2000 International Conference on Image Processing. Piscataway, NJ: IEEE, 2000: 690-693.
- [7] 李雷达,郭宝龙,表金峰. 基于奇偶量化的空域抗几何攻击图像水印算法[J]. 电子与信息学报, 2009, 31(1): 134-138.
- [8] 苗锡荣,孙劲光,张语涵. 图像归一化与伪Zernike矩的鲁棒水印算法研究[J]. 计算机应用研究, 2010, 27(3): 1052-1054.
- [9] 何冰,王珏,赵杰. 基于不变矩的抗旋转、缩放、平移鲁棒性数字水印[J]. 计算机工程与应用, 2010, 46(1): 183-186.
- [10] 赵,杰,王,珏,何冰. 基于Tchebichef矩和小波提升的数字水印算法[J]. 计算机工程, 2009, 35(11): 113-115.
- [11] 谢荣生,刘承香,杨树国,等. 基于模板匹配的抗几何攻击图像数字水印[J]. 哈尔滨工程大学学报, 2002, 23(3): 54-58.
- [12] 王丽,赵媛媛,赵耀. 一种抗剪切的鲁棒数字水印[J]. 数据采集与处理, 2006, 21(3): 330-333.
- [13] PEREIRA S, RUANAIDH J, DEGUILLAUME F, et al. Template based recovery of fourier-based watermarks using log-polar and log-log maps [C]// IEEE International Conference on Multimedia Computing and Systems. Piscataway, NJ: IEEE, 1999: 870-874.
- [14] 韩亚丹. 基于特征的抗剪裁数字水印技术研究[D]. 大连: 辽宁师范大学, 2006.
- [15] 邓峰森,王炳锡. 基于特征点的抗几何失真数字图像水印[J]. 信号处理, 2005, 21(1): 12-16.
- [16] CHOTIKAKAMTHORN N, PANTUWONG N, YAWAI W. Projective invariant digital image watermarking technique using four coplanar feature points [C]// IEEE International Conference on Image Processing. Piscataway, NJ: IEEE, 2005: 1005-1008.