

基于 SIFT 的 DCT 域抗几何攻击水印算法

郝荣霞, 彭玉忠

(潍坊医学院 计算机教研室, 山东 潍坊 261053)

摘要: 针对几何攻击的特点, 提出一种基于 SIFT 变换的鲁棒水印算法。嵌入过程中, 在图像的兴趣区域寻找合适的关键点, 利用交流系数关系在 DCT 域重复嵌入水印。提取过程充分利用 SIFT 关键点对旋转、尺度缩放等的不变性, 对隐秘图像进行校正, 找出水印嵌入位置, 并提取水印, 与原始水印进行相似度判定。实验结果表明, 基于 SIFT 变换的水印算法对常见几何攻击有较强的鲁棒性。

关键词: 数字水印; 几何攻击; 尺度不变特征变换; 离散余弦变换; 关键点

中图分类号: TP391

文献标识码: A

文章编号: 1674-7720(2010)14-0049-04

Geometrical attack robust watermark algorithm of DCT field based on SIFT

HAO Rong Xia, PENG Yu Zhong

(Staff Room of Computer, Weifang Medical College, Weifang 261053, China)

Abstract: According to the characteristics of geometric attacks, this paper offers a robust watermark algorithm based on SIFT. Look for appropriate key points in the ROI of image and repeatedly embed watermark in DCT field using AC relations in the embedding produce. Use the SIFT characteristics of invariant to rotation and scale zoom, correct the watermarked image, find out the location of watermark embedded, seek out watermark and decide similarity with origin watermark. Experiments show that watermark algorithm based on SIFT is robust to ordinarily geometric attacks.

Key words: digital watermark; geometrical attack; SIFT; DCT; key points

数字水印是实现版权保护的有效手段, 已成为信息安全领域的一个研究热点^[1]。目前, 鲁棒数字水印算法有了很大的发展, 而几何攻击有其固有的特点, 如对图像采用偏移、旋转、挤压、裁剪、扭曲、移去或插入像素及像素块等操作, 大量水印算法不能经受上述攻击, 因为几何变换使得水印检测位置偏离, 水印检测器必须知道水印嵌入的确切位置。若水印算法的设计没有明确用来抵御这种攻击, 则对这种攻击的补偿是困难的, 主要困难在于载体数据中对原始水印参考点的寻找。

几何变换不变性分析方法主要有互相关分析、傅里叶描述子、不变矩提取、自回归模型和基于小波的几何不变性分析等。目前, 许多学者已经做了很多有关几何变换不变性的研究。王暉在参考文献[2]中分别对图像几何变换不变性和纹理旋转不变性进行了研究和总结, 提出了一种基于 Radon 和解析 Fourier-Mellin 变换的尺度与旋转不变目标识别算法, 取得了很好的效果, 但其计算复杂度较高。何利英等提出了一种抗几何失真的彩色图像水印算法^[3], 利用彩色图像中蓝、绿分量小波系数间的关系, 在蓝色水平和垂直细节中嵌入相同的水

印, 利用红色分量中的 SIFT 特征点估计几何参数, 校正失真水印图像。

并在尺度不变特征变换 SIFT 由 LOWE D G 于 1999 年提出, 并在 2004 年进行了完善总结。SIFT 特征是图像的局部特征, 对旋转、尺度缩放、亮度变化保持不变, 对视角变化、仿射变换、噪声也保持相当程度的稳定^[4]。SIFT 变换信息量丰富, 匹配准确, 即使少数的几个物体也可以产生大量 SIFT 关键点, 应用前景非常广阔。

利用 SIFT 变换的旋转、尺度不变性, 结合图像鲁棒水印思想^[5-7], 本文提出了一种基于 SIFT 的离散余弦变换域抗几何攻击水印算法, 充分利用 SIFT 变换中关键点的独特性和匹配的稳定性、变频域数字水印鲁棒性好等特点, 较好地实现了抗几何攻击的水印算法。

1 SIFT 变换

SIFT 变换的主要步骤如下:

(1) 检测尺度空间极值点。对同一幅图像用不同的尺度表达, 利用不同尺度的高斯差分核与图像卷积检测稳定的关键点, 比较高斯差分图像中每个像素与其 26 个近邻像素的值是否为极值点, 以确定可能的 SIFT 关键

点。

(2)精确定位极值点。舍弃可能的关键点中低对比度的点和边缘点。

(3)为每个关键点指定方向参数。在以关键点为中心的邻域窗口内采样,利用直方图确定关键点处邻域的方向,作为关键点的主方向。

(4)关键点特征向量的生成。将坐标轴旋转为关键点的主方向,确保旋转不变性,再以关键点为中心取 16×16 的窗口,形成 1×128 维的SIFT特征向量。将特征向量归一化,去除光照变化的影响。

(5)关键点匹配。取图像A中的某个关键点,找出其与图像B中欧氏距离最近的前两个关键点,如果最近的距离除以次近的距离少于某个比例阈值,则认为图像A中的这个关键点与图像B中欧氏距离最近的关键点匹配。降低这个比例阈值,匹配点数目会减少,但更加稳定。

图1是两幅图像SIFT关键点匹配结果示意图,可以看出,虽然用于匹配的两幅图像的尺度、旋转角度等差别较大,但匹配效果很好,利用这一点,可以很好地定位受攻击的隐秘图像中水印的嵌入位置。

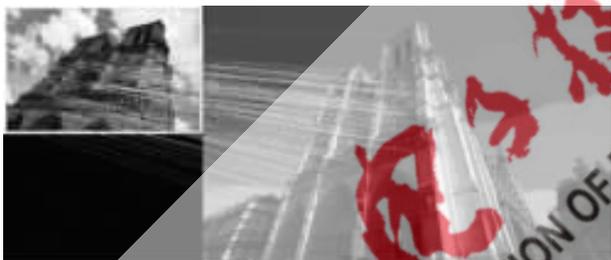


图1 SIF 关键点匹配结果示意图

2 水印算法

2.1 兴趣区域选择

图像信息有其自身的特点,因为图像数据的意义是基于内容的,与数据流无关。从图像数据意义的本质出发,把对理解图像内容最有意义的区域称为兴趣区域ROI(Region of Interests)。人们对图像的理解,通常是通过把图像按照某些特性(如灰度级、频谱、纹理等)划分成一些区域,然后基于划分的区域进行理解。攻击者为了保证图像的可用性,对关键兴趣区域的攻击强度较小,使得这些区域的水印保留可能性大大增加。

在许多图像应用中,对数据流的操作并不会引起图像内容的改变。为此,把水印全部或大部分嵌入在兴趣区域,舍弃语义上不重要的区域。如兴趣区域受到攻击,很容易使图像的视觉效果产生明显的改变而失去价值。因此,选择兴趣区域嵌入水印可以很好地提高水印的不可见性和嵌入强度。

例如,对图2所示的原始图像选择兴趣区域,结果如图3所示。兴趣区域的形状任意,但应避免图像的边界。

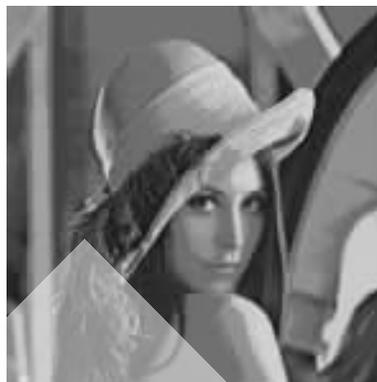


图2 lena 原始图像



图3 图2的兴趣区域

2.2 算法流程

2.2.1 嵌入算法流程

(1)对原始图像手动选择兴趣区域,如图3所示,利用二值图像进行标注,兴趣区域像素点用0表示,其余像素点用1表示,如图4所示。

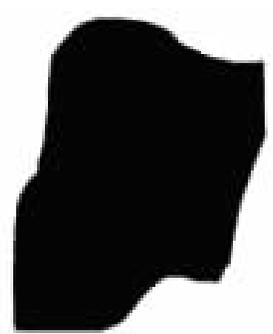


图4 图3对应的标注图像

(2)用SIFT算法提取兴趣区域内的关键点。关键点包含位置、尺度、方向3个信息,那些尺度较大或较小的关键点,对图像的尺度变化不稳定,被重新检测到的概率较小,因此,关键点尺度应位于某个范围内,一般在4~8之间。要求任意选定的关键点与其他已选定关键点的 8×8 邻域互不重叠,如图5所示。设二值水印 $W=(w_1, w_2, \dots, w_n)$ 的长度为 n ,不妨设 $n \bmod 8=0$,根据水印位嵌入方案,每个关键点邻域内嵌入8位水印,则提取的关

《微型机与应用》2010年第29卷第14期

图形、图像与多媒体

Image Processing and Multimedia Technology

关键点 p_1, p_2, \dots, p_m 的个数满足 $m \geq n/8$ 。令 $c = 8m/n$, c 为水印重复嵌入次数。



图5 兴趣区域内提取的SIFT关键点邻域

(3)用如下方法重复嵌入水印。其中,第 t 位水印重复嵌入到第 $d \times [n/8] + [(t-1)/8] + 1$ 个关键点邻域内, $d = (0, 1, 2, \dots, c-1), t = (1, 2, \dots, n)$ 。

将图像关键点的 8×8 邻域像素亮度矩阵 Y 做离散余弦变换 DCT 得到系数矩阵 X 。在 X 中按 Zigzag 顺序选择 6 和 7、8 和 9、10 和 11、13 和 14、12 和 24、15 和 16、17 和 18、19 和 20 共 8 对交流系数,用于嵌入 8 位水印。对嵌入第 i 位水印 $W_i (i=1, 2, 3, 4, 5, 6, 7, 8)$ 的两个交流系数 p_i^1, p_i^2 做如下调整:

如果第 i 位水印为 0, 判断 p_i^1, p_i^2 两个系数绝对值的关系, 如 $|p_i^2| - |p_i^1| \leq \frac{1}{2} \min(|p_i^1|, |p_i^2|)$, 令 $p_i^2 = \frac{3}{5}(|p_i^1| + |p_i^2|)$,

并保留原来的符号, 令 $p_i^1 = \frac{2}{5}(|p_i^1| + |p_i^2|)$, 并保留原来的符号;

如果第 i 位水印为 1, 判断 p_i^1, p_i^2 两个系数绝对值的关系, 如 $|p_i^1| - |p_i^2| \leq \frac{1}{2} \min(|p_i^1|, |p_i^2|)$, 令 $p_i^1 = \frac{3}{5}(|p_i^1| + |p_i^2|)$,

并保留原来的符号, 令 $p_i^2 = \frac{2}{5}(|p_i^1| + |p_i^2|)$, 并保留原来的符号;

对 X 做离散余弦反变换 IDCT 重新得到亮度矩阵, 此时, 图像关键点 p_j 的 8×8 邻域内已嵌入 8 位水印。

(4) 计算关键点 p_j 的特征向量 $\vec{k}_j (j=1, 2, \dots, m)$, 并保存为密钥文件 $K = [\vec{k}_1, \vec{k}_2, \dots, \vec{k}_m]$ 。

(5) 利用二值图像标注信息, 用嵌入水印的兴趣区域替换原始图像对应区域形成隐秘图像。

水印嵌入流程如图 6 所示。

2.2.2 提取算法流程

(1) 对受几何攻击的隐秘图像计算尺度因子在 4~8 之间的关键点特征向量表示为集合 $A = \{\vec{a}_1, \vec{a}_2, \dots, \vec{a}_m, \dots, \vec{a}_h\}$ 。

(2) 按照 SIFT 关键点匹配算法在 A 中找出与密钥文件中 \vec{k}_i 匹配的特征向量 \vec{a}_j , 所有被匹配的向量 \vec{a}_j 组成的集合记为 B , 如表 1 所示。记录匹配过程中与 \vec{k}_i 欧氏距离最近的关键点除以欧氏距离次近的关键点的比值。

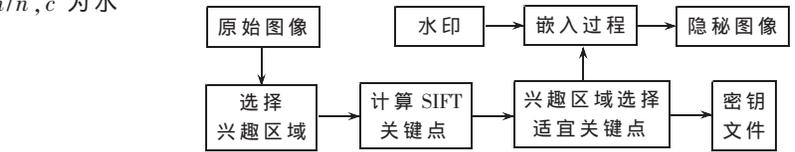


图6 水印嵌入流程图

表1 SIFT 关键点匹配结果示例

密钥文件 K	\vec{k}_1	\vec{k}_2	\vec{k}_3	\vec{k}_4	...	\vec{k}_m
集合 B	\vec{a}_3	\vec{a}_2	\vec{a}_5	无匹配	...	\vec{a}_h

(3) 根据步骤(2)关键点匹配过程中记录的比值, 选择比值最小的两对最优匹配关键点, 并保证两对最优匹配关键点之间有一定的距离, 按节 2.3 所述的方法对受攻击的隐秘图像进行几何失真校正, 得到校正后的隐秘图像, 同时校正集合 B 中匹配关键点的坐标。

(4) 用如下方法提取水印:

对关键点 8×8 邻域的亮度矩阵 Y' 做 DCT 变换, 得到系数矩阵 X' ; 从 X' 中选定用于提取第 i 位水印的两个交流系数 $p_i^1, p_i^2 (i=1, 2, 3, 4, 5, 6, 7, 8)$, 判断两个系数绝对值的关系, 如果 $|p_i^1| < |p_i^2|$, 则提取结果为 0; 如果 $|p_i^1| > |p_i^2|$, 则提取结果为 1。每个关键点邻域提取 8 位水印。

对用不同关键点重复嵌入的同一水印位计算平均值 w_j' , 最终提取的第 j 位水印为:

$$w_j = \begin{cases} 0 & (w_j' < 0.5) \\ 1 & (w_j' \geq 0.5) \end{cases}$$

(5) 用以下公式计算原始水印信号 $W = (w_1, w_2, \dots, w_n)$ 与提取的水印信号 $W' = (w_{11}', w_{21}', \dots, w_{n1}')$ 的相似度:

$$r(W', W) = \frac{\sum_{i=1}^n w_i w_i'}{\sqrt{\sum_{i=1}^n (w_i)^2} \sqrt{\sum_{i=1}^n (w_i')^2}}$$

若 $r(W', W) \geq T$, 可以判定被测图像中有水印存在, 否则, 没有水印, 其中 T 为门限值。一般认为, 当 $T=0.7$ 时, 便可认定水印的存在性。

水印提取流程如图 7 所示。

2.3 受几何攻击隐秘图像的旋转、缩放失真校正

由于隐秘图像受到攻击, 一些关键点不能在原始图像与受攻击隐秘图像间精确匹配, 为此, 在匹配的关键点集合内选择两对最优匹配关键点 $(P, P'), (Q, Q')$, 其中 $P(x_1, y_1), Q(x_2, y_2)$ 为原始图像的关键点坐标, $P'(x_1', y_1'), Q(x_2', y_2')$ 为受攻击的隐秘图像关键点坐标, θ 为受攻击的

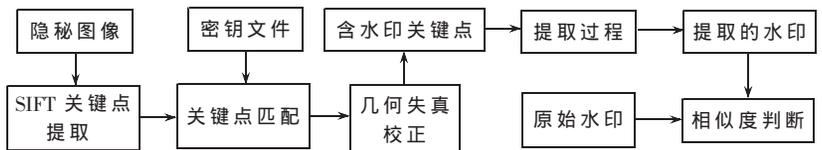


图7 水印提取流程图

隐秘图像相对于原始图像的旋转角度,则有:

$$\theta = \arctan \frac{y_2' - y_1'}{x_2' - x_1'} - \arctan \frac{y_2 - y_1}{x_2 - x_1}$$

如果 θ 为正,则表明隐秘图像逆时针旋转了 θ° ; 如果 θ 为负,则表明隐秘图像顺时针旋转了 θ° 。根据两关键点之间的位置关系,确定受攻击的隐秘图像相对于原始图像的缩放系数 α

$$\alpha = \frac{|x_2' - x_1'|}{|x_2 - x_1|} \text{ 或 } \alpha = \frac{|y_2' - y_1'|}{|y_2 - y_1|}$$

3 实验结果

实验一:水印嵌入和提取

对图 2 所示的 512 像素×512 像素标准 lena 图像进行测试,水印图像为 20 像素×20 像素的二值图像,如图 8 所示,共 400 个水印位。利用本文给出的算法嵌入水印,在兴趣区域选择 150 个关键点,如图 5 所示,每个关键点嵌入 8 位水印,因此,每个水印位重复嵌入 $150 \times 8 / 400 = 3$ 次。嵌入水印后的隐秘图像如图 9 所示。



图 8 水印图像



图 9 隐秘图像

隐秘图像逆时针旋转 45° 缩小为原图的 60%,如图 10(a)所示,几何失真校正后的图像如图 10(b)所示,对校正后的图像提取的水印如图 10(c)所示。



(a) 旋转及缩小



(b) 校正后图像



(c) 提取的水印

图 10 隐秘图像逆时针旋转及尺度缩小的校正实验

隐秘图像顺时针旋转 30° 放大 1.5 倍,如图 11(a)所示,几何失真校正后的图像如图 11(b)所示,对校正后的图像提取的水印如图 11(c)所示。

实验二:水印相似度测试

表 2 为图 11 所示的隐秘图像受到多种几何攻击后提取的水印与原始水印的相似度测试结果。

从以上实验可以看出,利用最优匹配关键点计算隐秘图像的几何失真并进行校正,可以很好地恢复隐秘图



(a) 旋转及放大



(b) 校正后图像



(c) 提取的水印

图 11 隐秘图像顺时针旋转及尺度放大的校正实验

表 2 水印相似度测试

所受攻击	相似度
无攻击	1.00
放大至 1.2 倍	0.91
放大至 1.5 倍	0.86
缩小至 0.7 倍	0.84
缩小至 0.9 倍	0.89
旋转 5°	0.95
旋转 30°	0.95
旋转 40° 再放大 1.2	0.90
旋转 30° 再缩小 0.9	0.85
边界剪切 20 像素	1.00
平移 20 像素	1.00

像。在隐秘图像丢失部分关键点信息即水印信息后,提取的水印图像有部分信息失真,水印相似度有所降低,但提取的水印图像内容可识别,水印相似度均大于水印相似门限值,表明算法可正确判定水印的存在,具有鲁棒性。

本文给出的基于 SIFT 的 DCT 域抗几何攻击水印算法,在原始图像选择兴趣区域,在关键点的 8×8 邻域嵌入 8 位水印,嵌入过程巧妙利用 DCT 域交流系数绝对值的关系表示水印位,利用 SIFT 关键点在隐秘图像和受几何攻击的隐秘图像间匹配的稳定性,确定匹配关键点,对受攻击隐秘图像的几何失真进行校正以正确提取水印。在变频域嵌入水印,提高了水印的鲁棒性。实验证明,本文的算法有效。

参考文献

- [1] MOULIN P, KOETTER R. Data-hiding codes. Proc. of the IEEE, 2005, 93(12): 2083-2126.
- [2] 王晖. 图像旋转与尺度变换不变性识别方法研究[D]. 西安:西安电子科技大学,2008.
- [3] 何利英,李智勇,刘伟灵.一种抗几何失真的彩色图像数字水印算法[J].计算机应用研究,2008,25(1):257-259.
- [4] LOWE D G. Distinctive image features from scale-invariant keypoints[J].International Journal of computer Vision, 2004,60(2):91-110.
- [5] BAS P, CHASSERY J M, MACQ B. Geometrically invariant watermarking using feature points[J].IEEE Transactions

on Image Processing, 2002,11(8):825-837.

(收稿日期:2010-04-07)

- [6] LEE H Y, KIM H S, LEE H K. Robust image watermarking using local invariant features[J]. Optical Engineering, 2006,45(3):91-110.
- [7] SEO J S, YOO C D, Image watermarking based on invariant regions of scale-space representation[J]. IEEE Trans. Signal Process, 2006,54(4):1537-1549.

作者简介:

郝荣霞,女,1979年生,讲师,硕士,主要研究方向:图像处理、信息安全。

彭玉忠,男,1971年生,副教授,硕士,主要研究方向:图像处理、信息安全。

