

基于 QR 码的抗几何攻击数字水印

白韬韬, 刘真, 卢鹏

(上海理工大学, 上海 200093)

摘要: 针对目前数字水印无法抵抗几何攻击的问题, 提出了一种基于 QR 码的抗几何攻击数字水印算法。将文字信息进行了 QR 码编码, 所得 QR 码作为水印信息。将载体图像进行一级离散小波变换, 在变换后的低频子图中分块嵌入了水印信息。实验结果表明, 本方法可以抵抗常见的旋转、等比例和不等比例缩放攻击, 同时对 JPEG 压缩也具有很好的鲁棒性, 此数字水印技术能够广泛应用到数字作品的版权保护中。

关键词: QR 码; 几何攻击; 离散小波变换

中图分类号: TS865 **文献标识码:** A **文章编号:** 1001-3563(2013)11-0113-04

Geometrical Attack Resistant Digital Watermarking Based on QR Code

BAI Tao-tao, LIU Zhen, LU Peng

(Shanghai University of Science and Technology, Shanghai 200093, China)

Abstract: A digital watermarking algorithm which can resist geometrical attack was proposed. Literal information was encoded as QR code. The QR code was embedded as a watermark into the low-frequency sub-block graph of the digital image by a discrete wavelet transform. Experiments demonstrated that this method can well resist attacks such as rotation, scaling and JPEG lossy compression. This digital watermarking technology can be widely used in copyright protection of digital works.

Key words: QR code; geometrical attack; discrete wavelets transform

随着网络和通信技术的快速发展, 数字图像、视频和音频等数字产品的版权保护越来越受到人们的重视, 数字水印技术是近年来学者们研究的热点, 也是解决数字产品版权问题比较有效的方法。衡量数字水印技术是否可靠的标准是其抵抗各种常见攻击的鲁棒性。但是, 数字水印技术还没有达到人们的要求。其中阻止水印技术走向应用的最主要问题就是水印技术能否有效抵抗几何攻击。

目前, 许多数字水印方法已经提出, 然而这些方法都不能有效的抵抗几何攻击。基于 Fourier-Mellin 变换^[2]的数字水印技术, 由于对数极坐标变换需要进行插值运算, 恢复后的图像产生很大的失真, 实用价值较低。基于模版匹配^[3]校正的数字水印技术, 可以一定程度上抵抗几何攻击, 但是由于方法复杂且计算量大, 实用性受到限制。基于图像特征点^[4]的数字水印技术, 由于算法复杂、特征点的数量过多、计算量大, 实用性较差。在空域中使用补丁(patchwork)算

法^[5]来解决水印同步问题, 但是这种算法及其复杂, 并且抵抗几何攻击的效果并不理想。本文利用与人眼视觉特性相适应的小波变换以及 QR 码的校正性能 and 纠错性能, 提出一种可以有效抵抗几何攻击的水印算法。该算法简单、计算量小且对图像质量影响较小, 有很强的实用性。

1 水印的嵌入方法

首先将信息进行编码生成 QR 二维码, 再对载体图像进行一级小波分解, 将低频子图分块, 把每个水印信息位嵌入到对应的子块中。利用上述方式把生成的 QR 码水印嵌入到低频子块的系数中。所用载体图大小为 $2M \times 2N$, 生成的 QR 码大小为 $m \times n$ 。具体步骤如下。

1) 载体图像进行一级 Haar 小波分解, 得到一个低频子图像 D_{LL} 和 3 个子图分别为水平方向系数

收稿日期: 2013-01-24

作者简介: 白韬韬(1989-), 男, 蒙古族, 辽宁锦州人, 上海理工大学硕士生, 主攻数字水印、图像处理。

D_{LL} , 垂直方向系数 D_{HL} , 对角线方向系数 D_{HH} 。四个子图的大小均为 $M \times N$ 。 (i, j) 表示低频子图的坐标, $D_{LL}(i, j)$ 表示低频子图的各个位置的系数。

2) 在 DWT 变换域的一级低频子块中嵌入 QR 码。将低频子图分成大小为 $M/m \times N/n$ 的子块, 共 $m \times n$ 个。将每一个水印信息位, 嵌入在对应的子块中。嵌入强度为 S , 当嵌入的水印信息位为 0 时:

$$D_{LL}(i, j) = \begin{cases} D_{LL}(i, j) - \text{mod}[D_{LL}(i, j), S] + \frac{S}{4} & 0 \leq \text{mod}[D_{LL}(i, j), S] < 3 \times S/4 \\ D_{LL}(i, j) - \text{mod}[D_{LL}(i, j), S] + S \times \frac{S}{4} & 3 \times S/4 \leq \text{mod}[D_{LL}(i, j), S] < S \end{cases}$$

当嵌入的水印信息位为 1 时:

$$D_{LL}(i, j) = \begin{cases} D_{LL}(i, j) - \text{mod}[D_{LL}(i, j), S] - \frac{S}{4} & 0 \leq \text{mod}[D_{LL}(i, j), S] < S/4 \\ D_{LL}(i, j) - \text{mod}[D_{LL}(i, j), S] + 3 \times \frac{S}{4} & S/4 \leq \text{mod}[D_{LL}(i, j), S] < S \end{cases}$$

3) 将嵌入水印的低频子图经过小波逆变换重构, 得到含有水印的图像。

2 水印的提取方法

1) 将含水印的图像进行一级小波分解, 得到图像的低频子图 D'_{LL} 。

2) 利用公式确定水印位, 公式如下:

$$\text{wmark}(i1, j1) = \begin{cases} 1 & \frac{S}{2} < \text{mod}[D'_{LL}(i, j), S] < S \\ 0 & 0 < \text{mod}[D'_{LL}(i, j), S] < \frac{S}{2} \end{cases}$$

3) 得到提取的 QR 码, 并将得到的 QR 码进行译码, 得到水印信息。

3 实验

用 1024×1024 像素大小的 lena 图像作为载体图像进行实验。设定水印信息为 deisldi 字符串, 将其编码为 QR 码, 纠错等级为 30%。再将 QR 码修改成 64×64 像素大小的图像。利用上述嵌入方法, 将载体图像按 8×8 大小分块, 嵌入水印得到含水印图像, 实验用图像见图 1。载体图像与含水印图像的 psnr 值为

38.92。



图 1 实验用图像

Fig. 1 Images for experiment

实验包括 3 部分: 第 1 部分为本方法单独抵抗旋转、缩放攻击的性能; 第 2 部分为本方法抵抗旋转、缩放复合攻击的性能; 第 3 部分检验本方法是否能够抵抗几何攻击与 JPEG 压缩的混合攻击。

3.1 第 1 部分

1) 旋转实验。将含水印图像在 matlab 中逆时针旋转 5.5° , 选择 nearest, bilinear 和 bicubic 三种插值方式分别进行旋转攻击, 然后再提取水印解码, 见表 1。

表 1 3 种插值方式的旋转攻击实验结果

Tab. 1 Experimental results of rotation attack with three methods of interpolation

旋转角度	插值方式	提取的水印	能否解码
5.5°	nearest		能
5.5°	bilinear		能
5.5°	bicubic		能

选择不同的插值方式是考虑在实际应用过程中, 无法预测图片的使用者在旋转缩放的过程中所采用的插值方式, 所以尽可能的对每种插值方式进行实验。

在 PS 中任意角度旋转含水印图像, 然后提取水印解码, 提取出的 QR 码可以解码, 见图 2。

2) 缩放实验。将含水印图像在 matlab 中进行缩



图2 任意角度旋转攻击实验

Fig.2 Experiment for attack of rotation

放,选择 nearest, bilinear 和 bicubic 3 种插值方式分别进行缩放攻击,然后再提取水印解码,见表 2。

表 2 3 种插值方式缩放攻击的实验结果

Tab.2 Experimental results of scaling attack with three methods of interpolation

缩放比例	插值方式	提取的水印	能否解码
等比例放大 1.5 倍	nearest		能
等比例放大 1.5 倍	bilinear		能
等比例放大 1.5 倍	bicubic		能
高度缩小为 0.9 倍, 宽度放大 1.6 倍	nearest		能
高度缩小为 0.9 倍, 宽度放大 1.6 倍	bilinear		能
高度缩小为 0.9 倍, 宽度放大 1.6 倍	bicubic		能

在 PS 中任意比例缩放(长、宽不超过 3 倍)含水印图像,然后提取水印解码,提取出的 QR 码可以解码,见图 3。



图3 任意比例缩放攻击实验

Fig.3 Experiment for attack of scaling

3.2 第 2 部分

将含水印图像在 matlab 中进行旋转、缩放组合攻击,选择 nearest, bilinear 和 bicubic 3 种插值方式分别进行组合攻击,然后再提取水印解码,见表 3。

表 3 三种插值方式的旋转、缩放组合攻击实验结果

Tab.3 Experimental results of combination attack with three methods of interpolation

旋转角度及 缩放比例	插值 方式	提取的 水印	能否 解码
旋转 9.3°, 宽度缩小为 0.9 倍, 高度放大 1.2 倍	nearest		能
旋转 9.3°, 宽度缩小为 0.9 倍, 高度放大 1.2 倍	bilinear		能
旋转 9.3°, 宽度缩小为 0.9 倍, 高度放大 1.2 倍	bicubic		能

在 PS 中任意旋转、缩放含水印图像,然后提取水印解码,提取的 QR 码可以解码,见图 4。



图4 任意旋转、缩放组合攻击实验

Fig.4 Experiment for combination attack of rotation and scaling

3.3 第 3 部分

在第 2 部分实验的基础上,进行 JPEG 压缩攻击

实验,检验本方法抵抗几何变换和 JPEG 压缩的混合攻击性能。实验选择第二部分中,在 PS 中任意旋转、缩放的图片进行压缩实验,再提取水印,进行解码,见表 4。

表 4 JPEG 压缩攻击实验结果

Tab.4 Experimental results for attack of JPEG compression

JPEG 压缩的质量因子	提取的水印	能否解码
90%		能
80%		能
70%		能
60%		能

实验表明,应用 nearest、bilinear 和 bicubic 3 种插值方式进行实验,含水印图像经过包括旋转、等比例缩放和不等比例缩放的几何攻击后,提取出的 QR 码水印信息,虽然几何形态也发生变化,但是均可进行解码。第三部分的实验也证明,本方法可以抵抗一定的几何变换与 JPEG 压缩的混合攻击,且鲁棒性较强。

4 结论

提出了一种基于 QR 码的抗几何攻击数字水印算法。该算法将含水印图像经过离散小波变换得到的低频系数进行分块,再量化嵌入水印信息,提高了水印的稳定性和鲁棒性。同时将 QR 码作为水印信息,利用 QR 码自身的校正性能和纠错性能进一步提高了水印的鲁棒性。设计仿真实验证明了本算法有较强的抗几何攻击和 JPEG 压缩攻击的能力,在几何变换的过程中分别采用 3 种插值方法进行实验,均可

解码提取水印信息。同时由于本算法属于盲水印,在提取水印时不需要借助原图像,所以本文所提的数字水印技术有很强的应用前景。

参考文献:

- [1] 王子煜,孙刘杰,李孟涛. 强鲁棒性 QR 码水印技术[J]. 包装工程,2012,33(15):84-87.
WANG Zi-yu, SUN Liu-jie, LI Meng-tao. QR Code Watermark Technology with Strong Robustness [J]. Packaging Engineering, 2012, 33(15):84-87.
- [2] JOSEPH J K, RUANAIDH O, PUN T. Rotation, Scale and Translation Invariant Digital Image Watermarking[J]. Signal Processing, 1998, 66(3):303-317.
- [3] 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.
XIE Rong-sheng, LIU Cheng-xiang, YANG Shu-guo, et al. Geometrical Attack Resistant Digital Image Watermarking Based on Template Searching [J]. Journal of Harbin Engineering University, 2002, 23(3):54-58.
- [4] BAS P, CHASSERY J M, MACQ B. Geometrically Invariant Watermarking Using Feature Points [J]. Image Processing, 2002, 11(9):1014-1028.
- [5] BENDER W, GRUHL D, MORIMOTO N. Techniques for Data Hiding [R]. Cambridge: Massachusetts Institutes of Technology Media Lab, 1994.
- [6] 俞登峰,李学斌. 基于傅里叶-梅林变换的零水印算法[J]. 计算机工程与设计,2009,30(10):2566-2569.
YU Deng-feng, LI Xue-bin. Zero-watermark Algorithm Based on Fourier-Mellin Transforming [J]. Computer Engineering and Design, 2009, 30(10):2566-2569.
- [7] 肖菲菲,刘真. 二维码防伪技术在可变数据印刷中的应用[J]. 包装工程,2011,32(21):102-109.
XIAO Fei-fei, LIU Zhen. Application of Anti-counterfeiting Technology Based on Two-dimensional Bar Code in Variable Data Printing [J]. Packaging Engineering, 2011, 32(21):102-109.
- [8] 高发东,黎绍发,沈既武,等. 基于视觉和二维条形码的数字水印[J]. 计算机工程与应用,2003(28):28-31.
GAO Fa-dong, LI Shao-fa, SHEN Ji-wu, et al. Digital Watermarking Based on HVS and 2-Dimensional Bar Code [J]. Computer Engineering and Applications, 2003(28):28-31.