图文信息技术

抗缩放攻击的高水印容量数字水印算法

王潇，徐建刚
（南京大学 建筑与城市规划学院，南京 210093）

摘要：目的 为了增加水印算法的可嵌入水印信息容量，解决抗高强度缩放攻击等问题，提出一种基于圆形角度模板的抗缩放攻击、高水印容量的数字水印算法。**方法** 首先将原始水印信息转换为 QR 码，根据 QR 码生成原理提取其数据编码，并进行分组，再将分组的编码转换为角度信息；随机生成具有方向性和周期性的基础圆形模板水印，根据角度信息对其进行旋转，生成待嵌入的圆形角度模板水印；通过修改图像的最小可察觉误差完成水印信息的嵌入；通过检测模板水印中的角度信息，提出水印信息。**结果** 实验结果表明，该算法不仅可有效抵抗高强度的缩放攻击，同时还可以抵抗色彩调整、旋转、压缩、噪声、滤波、模糊等攻击。此外，该算法可实现较高容量的水印信息嵌入和无损提取。**结论** 通过对水印信息预处理和圆形角度模板水印的应用，不仅使得该算法具备高水印容量，而且可有效抵抗高强度缩放攻击，在抵抗色彩调整、旋转等图像处理攻击方面同样具备较强的鲁棒性，能满足实际应用需求。

关键词：QR 码；预处理；圆形角度模板；抗缩放攻击；高水印容量
中图分类号：TP391.4 **文献标识码：**A **文章编号：**1001-3563(2019)17-0216-11
DOI：10.19554/j.cnki.1001-3563.2019.17.032

High Capacity Digital Watermarking Algorithm against Scaling Attacks

WANG Xiao, *XU Jian-gang*
(School of Architecture and Urban Planning, Nanjing University, Nanjing 210093, China)

ABSTRACT: The work aims to propose a digital watermarking algorithm based on circular angle template for anti-scaling attack and with high watermark capacity, in order to improve the embeddable watermark information capacity of watermarking algorithm and solve the problem of high-intensity scaling attack. Firstly, the original watermark information was converted into a QR code. The data code was extracted according to the QR code generation principle, and then grouped and converted into angle information. Secondly, a basic circular template watermark with directionality and periodicity was randomly generated. Then, it was rotated according to the angle information to generate a circular angle template watermark to be embedded. Thirdly, the embedding of the watermark information was completed by modifying the just noticeable distortion (JND) of the image. Finally, the watermark information was extracted by detecting the angle information in the template watermark. The experimental results showed that, the proposed algorithm could not only effectively resist high-intensity scaling attacks, but also resist color adjustment, rotation, JPEG compression, noise, filtering and blurring. In addition, the algorithm could achieve the embedding and lossless extraction of higher capacity watermark information. Through the application of watermark information preprocessing and circular angle template watermarking, the watermarking algorithm not only has high watermark capacity, but also can effectively resist high-intensity anti-scaling

收稿日期：2019-05-29
基金项目：国家自然科学基金（51778278，51278239）
作者简介：王潇（1994—），女，博士，主要研究方向为信息安全、数字城市规划技术。
通信作者：徐建刚（1960—），男，南京大学教授、博导，主要研究方向为数字城市规划技术。

attacks. In addition, it also has strong robustness against image processing attacks such as color adjustment and rotation, which meets the needs of practical applications.

KEY WORDS: QR code; preprocessing; circular angle template; anti-scaling attack; high watermark capacity

数字图像具有方便编辑、传输和存储等特点，在新闻、社交和旅游等方面具有广泛应用。在移动互联网时代，互联网的发展在给图像分享提供便利的同时，也会出现图像被恶意篡改、盗用和非法拷贝等一系列问题。数字水印作为一种信息安全技术，能够在数字化产品中嵌入水印信息，从而可以为图像的防伪溯源、版权保护等提供技术手段[1]。图像数字水印技术的研究主要集中在空间域[2—4]、变换域[5—8]和特征域[9—12]，数字水印技术也从第 1 代全局水印的思想逐步向第 2 代特征区域水印转变。更高的不可感知性和更强的鲁棒性成为构建数字水印算法的新要求和目标。

随着互联网技术的迅猛发展，网络传输取代了传统的磁盘拷贝，成为当下首选的数据传播途径，然而为了提升网络传输速率，数据在传输过程中被大幅度缩放和压缩。高强度缩放作为网络有损传输中最常见的操作，在为数据传播带来便利的同时也为数据安全构成新的威胁。抗高强度缩放攻击成为研究抵抗网络有损传输的关键。目前，抗缩放攻击的水印算法集中在图像特征不变量的研究上，以差分特征点网格[13—14]和特征算子[15—16]研究较多。由于该类算法难以抵抗高强度的缩放攻击，在面临高强度攻击时，特征点易被破坏，因此难以实现水印的精准检测。

此外，水印信息的嵌入数据量直接影响水印算法的不可感知性，以较少的嵌入量表示较多的水印信息是提高算法不可感知性的切实可行的途径。QR 码作为一种矩阵二维码，具有可靠性高、占用空间小、纠错性能强等优点，被广泛应用于数字水印算法中[17—19]。关于 QR 码水印信息预处理已经取得一些研究成果[20—21]，但仍存在信息冗余度高的问题，QR 码水印信息预处理仍值得被探究。

文中通过深入分析 QR 码的生成机制，以 QR 码的数据编码取代 QR 码，结合角度编码达到高水印容量的目的；之后通过构建具有角度特征的模板水印，将水印信息以更加稳健的方式嵌入数字图像，提出一种抗缩放攻击的高水印容量数字水印算法，为解决抗高强度缩放攻击、提升水印容量等问题提供可行的技术途径。

1　水印信息预处理

1.1　QR 码预处理

QR 码（Quick Response Code）是目前被广泛使用的一种正方形阵列二维码，据 GB/T18284—2000《快速响应矩阵码》[22]可知，QR 码由数据及纠错编码、格式信息和功能图形构成，其中功能图形包括空白区域，位置探测图形及分隔符，定位及校正图形。QR 码符号结构（版本 2）见图 1。

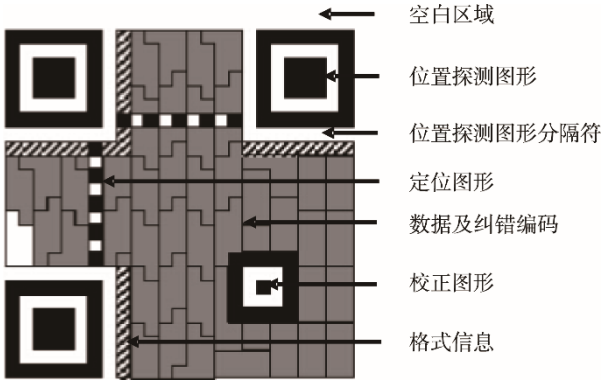


图 1　QR 码的符号结构（版本 2）
Fig.1 QR code symbol structure (Version 2)

相较于常见的水印信息生成方式（文本水印信息和图片水印信息），QR 码在水印容量、嵌入数据量以及鲁棒性等方面具备显著优势，因此，文中将 QR 码作为水印信息的生成方式。

为提升 QR 码作为水印信息生成方式的优势，文中基于国家标准《快速响应矩阵码》，通过对 QR 码进行预处理，减少 QR 码的冗余信息，以达到高强度压缩 QR 码、提高水印容量等目的。具体操作流程如下所述。

1）生成 QR 码信息。根据原始水印信息量选择合适的 QR 码版本及模块数生成 QR 码，并根据模板数 n，读取有用的信息部分，此时水印信息数量为原来的 $1/(n\times n)$ 倍。

2）提取 QR 码数据码字。根据 QR 码的编码过程将其逆推，提取 QR 码数据编码部分，将其他诸如纠错码字及固定部分等冗余信息去除。其水印信息记为 $W_0=\{0,1\}$，此时 QR 码得到大幅度的压缩。

3）生成待嵌入水印信息。QR 码的数据编码信息即为待嵌入的水印信息。

1.2　水印信息转角度信息

为了进一步提高水印信息容量，文中对上述待嵌入的 QR 码水印信息继续处理，使其水印信息得到进一步压缩。主要思路：在保证水印信息检测准确度的前提下，将待嵌入的水印信息进行编码，之后将其转换成角度信息。具体操作流程如下所述。

1）读取 QR 码数据编码。将待嵌入的 QR 码水印信息转为一维数组，$W=\{W_i, i=0,1,2\cdots L\}$，其中 $W_i\in\{0,1\}$，水印长度为 L。

2）对每 4 位一组的水印进行编码。此时水印信息 $W^{'}=\{W_i^{'}, i=0,1,2\cdots l\}$，其中 $W_i^{'}\in\{0,1\}$，水印长度 $l=L/4$。

3）基于半圆机制的角度编码。半圆机制的角度个数取 $n=16$，角度间隔为 11.25°，见图 2。为便于嵌入和检测水印信息，文中选取角度区间中值（取整）作为该区间对应的水印信息。

如水印信息“0000”对应的角度区间为 $[0,11.25°]$，即该区间中值 6°表示水印信息“0000”。

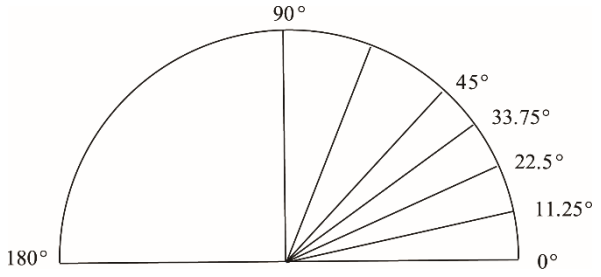


图 2　角度区间划分
Fig.2 Angle interval division

2　算法设计

2.1　算法思想

为解决抗高强度缩放攻击等问题，文中摒弃了水印算法中以 0/1 二值序列嵌入水印的思想，通过构建具有角度信息的圆形模板，完成水印的嵌入；在水印信息检测过程中，通过检测圆形模板中的角度信息得到水印信息。相较于 0/1 二值水印信息的嵌入，该方法的优点在于：当含水印图像受到不同程度的攻击破坏时，其图像像素值被大幅度破坏，但仍能通过检测模板水印中的角度信息进而提取原始水印信息。基于此，文中构建了一种基于圆形角度模板的强鲁棒性数字水印算法。

文中算法需要解决的关键技术问题：圆形角度模板水印的构建，采用含有角度信息的圆形模板水印替代二值序列水印信息是增强水印算法鲁棒性的关键，圆形角度模板水印的构建则成为首要解决的关键问题；角度检测，从角度模板中准确检测角度信息成为提取水印的关键，增强检测角度模板中直线斜率的准确性成为有待解决的问题。

2.2　圆形角度模板水印构建

基本步骤如下所述。

1）任意生成一个方形模板水印块 $W_0(x,y)$，通过垂直和水平方向的平移，使其具有方向性和周期性，见图 3a。

2）根据方形模板水印块 $W_0(x,y)$ 得到基础圆形模板水印 $W(x,y)$，见图 3b。

3）依据角度信息 θ，通过旋转 $W(x,y)$，生成圆形角度模板水印 $W^{\theta}(x,y)$，使其包含角度信息，见图 3c，此时 θ=45°。

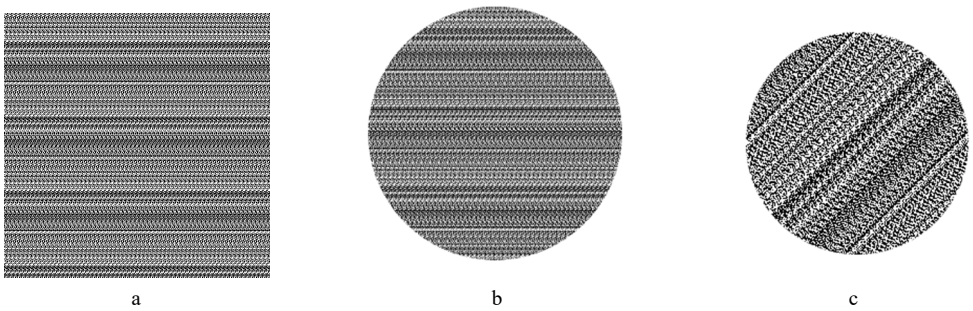


图 3　圆形角度模板构建
Fig.3 Circular angle template construction

2.3　水印嵌入

水印信息的嵌入规则是结合最小可察觉误差（Just Noticeable Distortion，JND），通过改变原始图像蓝色通道像素值完成嵌入。由于人眼视觉系统对于红、绿、蓝三通道的色彩敏感程度不同，其中对蓝色通道色彩感知能力最差，因此文中将水印信息嵌入蓝色通道，以增强水印算法的不可见性，减少水印信息对原始图像的视觉质量影响。

水印信息嵌入算法流程见图 4。

水印信息嵌入步骤如下所述[23]。

1）获取原始图像蓝色通道像素值及尺寸大小。读取原始图像，其尺寸记为 $M\times N$，并获取蓝色通道像素值 $B(x,y)$。

2）计算原始图像的 JND 值。其中，最小可察觉误差 $JND(x,y)$ 由两部分共同得到，分别是亮度 JND 模型和纹理 JND 模型。

3）原始图像分块。为保证每一位水印信息均可嵌入至原始图像中，现根据圆形角度模板水印的块数

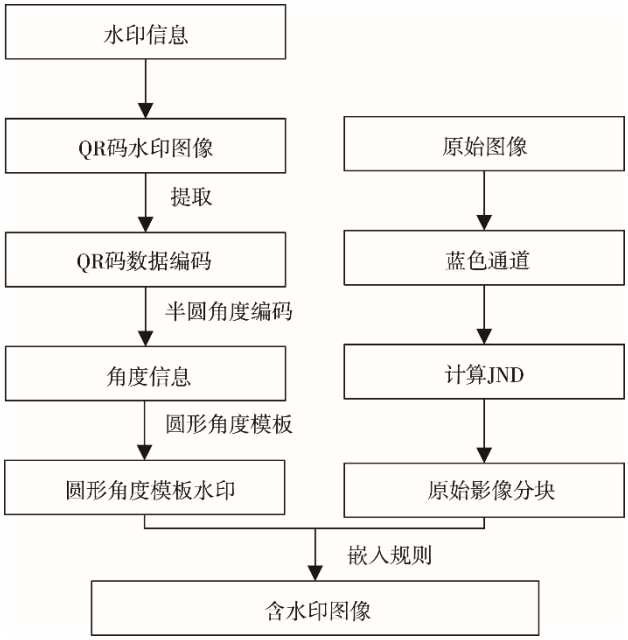


图 4　水印信息嵌入流程
Fig.4 Embedding process of watermark information

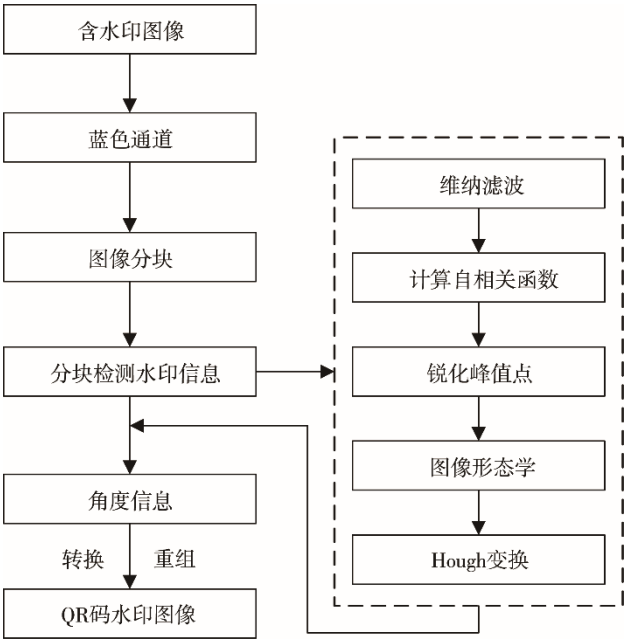


图 5　水印信息检测流程
Fig.5 Detection process of watermark information

l，将原始图像进行分块，分块数为 $\frac{M}{l}\times\frac{N}{l}$。

4）水印嵌入规则。将 $W^{\theta}(x,y)$ 嵌入载体图像中，得到含水印图像。

$$B_i^{'}(x,y)=B_i(x,y)+10\times\delta\times JND(x,y)\times W^{\theta}(x,y)+\delta\times\left(1-JND(x,y)\right)\times W^{\theta}(x,y) \tag{1}$$

式中：$B_i(x,y)$ 为第 i 个分块蓝色通道像素值；$B_i^{'}(x,y)$ 为嵌入水印之后第 i 个分块蓝色通道像素值；δ 为水印强度。

2.4　水印检测

常见水印算法采用“水印检测即为水印嵌入逆过程”的操作方式，这里通过提取模板水印中蕴含的角度信息来得到相应的水印信息。水印信息嵌入算法流程见图 5。

水印信息检测步骤如下所述[24]。

1）获取含水印图像蓝色通道像素值及尺寸大小。读取含水印图像，其尺寸记为 $M^{'}\times N^{'}$，并获取蓝色通道像素值 $B^{'}(x,y)$。

2）分块检测水印信息。采用维纳滤波去除噪声；计算自相关函数；锐化峰值点；引入图像形态学知识突显峰值点；通过 Hough 变换提取角度。

3）角度信息解码。根据角度所处的区间范围，得到相应的水印信息。

4）QR 码重组。依据 QR 码生成原理和步骤 3）得到的水印信息，计算纠错编码部分，并与固定结构部分进行重组，得到完整的 QR 码。

3　实验与分析

为了验证文中算法的鲁棒性和实用性，分别从不可见性分析、鲁棒性实验及算法对比实验等 3 个方面展开。

水印信息为“实验数据为 XX 省 XX 大学 XX 学院所有使用期间禁止非法复制传播盗版必究”，将上述包含 31 个汉字的文本水印信息编码成版本为 4，纠错级别为 M，模块数为 2，尺寸大小为 66×66 的 QR 码。QR 码水印图像见图 6。经第 1 节水印信息预处理之后，水印信息大小仅为 128 位，水印信息压缩至原来的 2.94%。

图 6　QR 码水印图像
Fig.6 QR code watermark image

实验中选取数字图像处理常用数据集 CSet12 中的 8 幅彩色图像作为实验数据，其数据格式为.jpg，尺寸为 1024×1024，见图 7。

实验中，在保证水印检测准确度的前提下，将原始图像的分块数定为 16×16，水印嵌入强度 δ=10，此时可嵌入的水印容量为 1024 位。原始数据为

1024×1024 时，结合第 1 节水印信息预处理内容，此时水印信息可容纳 65 个汉字或者 255 个数字等，能够满足实际应用需求，达到高水印容量的目的。水印信息容量由原始数据的尺寸决定，原始图像尺寸越大，可嵌入的水印容量越高。

3.1　不可见性实验

嵌入水印后的图像和提取出的水印信息见图 8。

为验证文中算法的不可见性，将从主观视觉和客观评价等 2 个方面展开。主观视觉通过人眼主观感受

图 7　原始图像

Fig.7 Original image

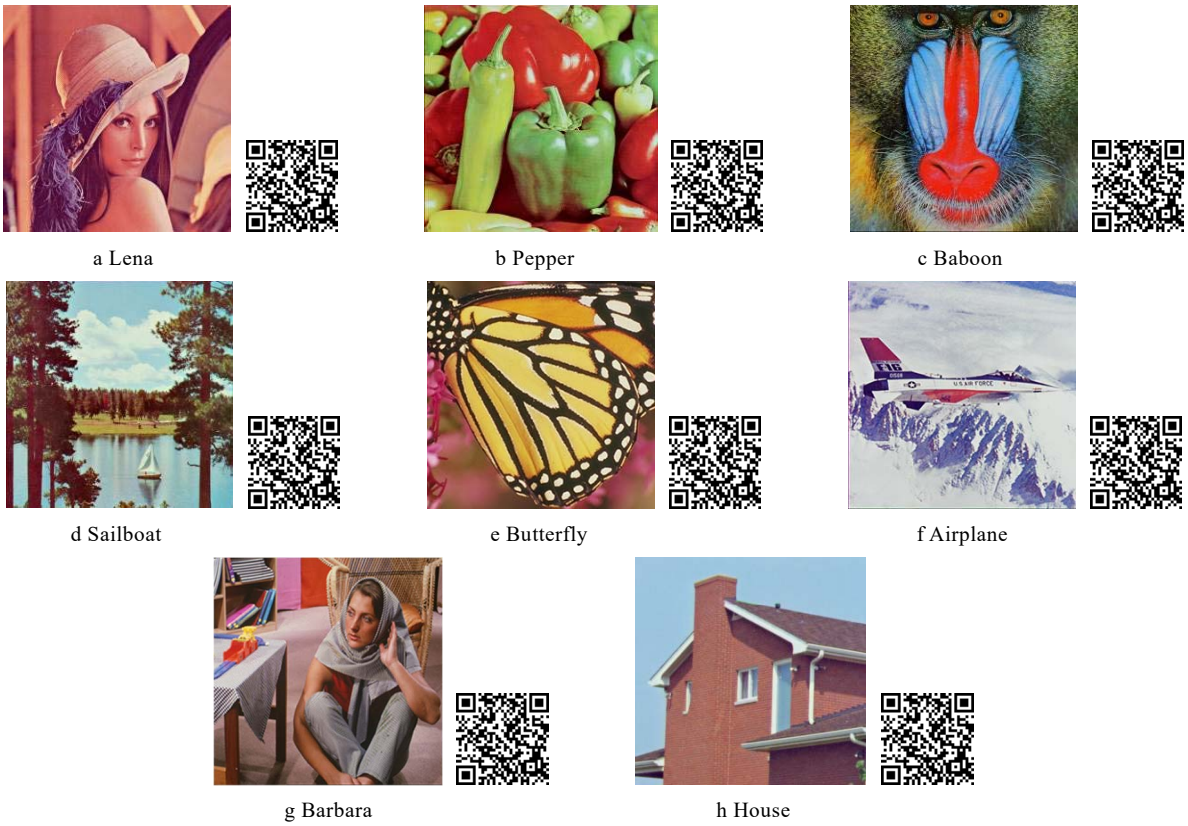


图 8　含水印图像和提取的 QR 码水印图像

Fig.8 Watermark image and extracted QR code watermark image

判断，客观评价通过参数指标进行评价。参数指标选取峰值信噪比（PSNR）、相关系数（NC）和位错率（BER），PSNR 用于评价原始图像与含水印图像之前的质量差别；NC 和 BER 用于评价提取的水印信息与原始水印信息之间的差别。

将图 7 和图 8 的 4 幅图像进行对比观察，从主观视觉可知，看不出原始图像在嵌入水印前后的差异。由表 1 可知，从 4 幅含水印图像中提出的水印信息均与原水印信息的相关系数为 1，位错率为 0，表明在不遭受任何攻击的前提下，水印信息能够被完整无损地检测。嵌入水印前后所计算出的峰值信噪比均大于经验阈值 28，从定量评价指标上可以充分说明采用文中算法嵌入水印后图像的质量没有明显下降。

表 1 不可见性定量评价

Tab.1 Quantitative evaluation of invisibility

实验数据	相关系数	位错率	信噪比
Lena	1	0	39.342
Pepper	1	0	40.097
Baboon	1	0	39.758
Sailboat	1	0	42.786
Butterfly	1	0	41.352
Airplane	1	0	38.093
Barbara	1	0	42.436
House	1	0	40.034

3.2　鲁棒性实验

为验证文中算法的鲁棒性，将从缩放攻击、色彩调整攻击、旋转攻击以及多种常规图像攻击等 4 个方面进行分析。

1）缩放攻击实验。放大和缩小会造成图像插值和重采样，引起图像像素值的改变，水印信息在遭遇缩放攻击时易被破坏。文中通过对 4 幅含水印图像进行不同程度的放大和缩小攻击，并对遭受缩放攻击之后的含水印图像进行水印信息的提取，部分实验结果见表 2（注：8 幅数据中选取信噪比较低的 4 幅数据显示其结果，下同）。由表 2 结果可知，文中算法可有效抵抗缩放因子从 0.25 到 10 范围内的高强度缩放攻击。1024×1024 的含水印图像，在缩小到 256×256 大小时，检测的水印位错率为 0，表明水印信息被无损检测；当放大至 10240×10240 时，水印信息同样被完整提取。可见文中算法抵抗缩放攻击效果显著，具有较强的鲁棒性和实用性。

表 2　缩放攻击实验结果

Tab.2 Experimental results of scaling attack

缩放因子	10	5	2	0.75	0.5	0.25
Lena						
尺寸	10240×10240	5120×5120	2018×2018	768×768	512×512	256×256
位错率	0	0	0	0	0	0
扫描结果	实验数据为XX省XX大学XX学院所有使用期间禁止非法复制传播盗版必究					
Baboon						
尺寸	10240×10240	5120×5120	2018×2018	768×768	512×512	256×256
位错率	0	0	0	0	0	0
扫描结果	实验数据为XX省XX大学XX学院所有使用期间禁止非法复制传播盗版必究					
Airplane						
尺寸	10240×10240	5120×5120	2018×2018	768×768	512×512	256×256
位错率	0	0	0	0	0	0
扫描结果	实验数据为XX省XX大学XX学院所有使用期间禁止非法复制传播盗版必究					
House						
尺寸	10240×10240	5120×5120	2018×2018	768×768	512×512	256×256
位错率	0	0	0	0	0	0
扫描结果	实验数据为XX省XX大学XX学院所有使用期间禁止非法复制传播盗版必究					

2）色彩调整攻击实验。在图像增强过程中，经常通过色彩调整的方式实现，色彩调整会造成图像像素值大幅度改变，水印信息容易被破坏。亮度和对比度调整作为图像色彩调整常见的操作方式，对图像像素破坏较大，具有较强的攻击性[25—26]。为验证文中算法对色彩调整攻击的鲁棒性能，通过同时改变图像的亮度和对比度进行实验，部分实验结果见表 3。由表 3 可知，文中算法对色彩调整攻击具备较好的鲁棒性。当含水印图像遭遇色彩调整攻击时，其像素值较原始像素值改变较大，但水印信息仍能被无损检测，位错率为 0，表明该算法能够有效抵抗色彩调整攻击。

3）旋转攻击实验。作为几何攻击之一，旋转攻击会造成图像发生重采样，使得像素值改变，水印信息易被破坏。为验证本算法抵抗旋转攻击能力，对实验数据进行一定角度范围内的旋转攻击实验，部分实验结果如表 4 所示。由表 4 可知，文中算法可抵抗角度在[−10°,10°]范围内的旋转攻击，水印信息被无损提取，位错率为 0。这是由于文中算法通过检测角度所属区间进而确定水印信息，保证了算法的容错性，使得算法能够抵抗一定范围的旋转攻击。

4）常规图像攻击实验。为验证算法对常规图像处理方式的鲁棒性，分别对含水印图像进行 JPEG 压缩、椒盐噪声、高斯噪声、中值滤波、均值滤波、高斯模糊等处理。以图 6a（Lena）为例进行实验，实验结果见表 5。由表 5 可知，文中算法可抵抗 JPEG 压缩、噪声、滤波和模糊等常规图像攻击。且提取的 QR 码水印信息位错率均为 0，QR 码能够被完整提取，表明该算法水印信息的强稳健性较难被破坏。

3.3　算法对比实验

为验证文中算法的抗缩放攻击能力，将文中算法与 2 类较为经典的抗缩放攻击水印算法进行对比分

表 3　色彩调整攻击实验结果

Tab.3 Experimental results of color adjustment attack

(亮度,对比度)	未攻击图像	(100, 50)	(50, 25)	(-50, -25)	(-100, -50)
Lena					
Baboon					
Airplane					
House					
尺寸	1024×1024	1024×1024	1024×1024	1024×1024	1024×1024
位错率	0	0	0	0	0
提取的QR码					
扫描结果	实验数据为XX省XX大学XX学院所有使用期间禁止非法复制传播盗版必究				

表 4　旋转攻击实验结果

Tab.4 Experimental results of rotating attack

旋转	10°	5°	−5°	−10°
Lena				
Baboon				
Airplane				
House				
尺寸	1187×1187	1110×1110	1110×1110	1187×1187
位错率	0	0	0	0
提取的QR码				
扫描结果	实验数据为XX省XX大学XX学院所有使用期间禁止非法复制传播盗版必究			

表 5　常规图像攻击实验结果

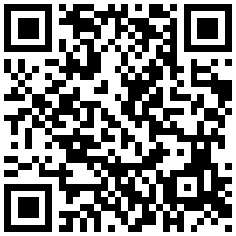
Tab.5 Experimental results of common image attack

攻击方式	JPEG压缩（因子4）	椒盐噪声（方差0.015）	高斯噪声（方差0.003）	中值滤波（模板3×3）	均值滤波（模板3×3）	高斯模糊（模糊半径1）
位错率	0	0	0	0	0	0
提取的QR码						
扫描结果	实验数据为XX省XX大学XX学院所有使用期间禁止非法复制传播盗版必究					

析。原始图像见图 9a，尺寸为 512×512；水印信息为“实验数据为 XX 省 XX 大学 XX 学院所有使用期间禁止非法复制传播盗版必究”，根据水印信息的内容，生成尺寸为 66×66 的 QR 码水印图像，见图 9b；同时将上述内容生成同等尺寸的文本水印图像，结果见图 9c。具体实验结果见表 6。

由表 6 可知，在水印嵌入数据量方面，文献[14]算法和文献[16]算法嵌入数据量均为 4356 bit，最大限度能表示 20 个汉字，而文中算法仅嵌入 128 bit，可表示 31 个汉字，表明文中算法可有效降低水印信息嵌入数据量，提高水印信息容量。在抗缩放攻击方面，文献[14]算法可有效抵抗缩放因子在 0.5~1.5 之间的缩放攻击，且放大缩小攻击均使得水印信息提取存在一定的位错率；文献[16]算法抗缩放攻击能力有所提升，可抵抗缩放因子在 0.5~2.0 之间的缩放攻击，放大攻击水印信息能够无损提取，缩小攻击水印信息提取有一定的位错率。相比之下，文中算法可有效抵抗缩放因子在 0.25~10 之间的缩放攻击，解决抗高强度缩放攻击的问题；同时，放大、缩小攻击均使得水印信息被无损检测，增强了算法的准确性。由此可见，文中算法在水印信息容量和抗缩放攻击等方面具有明显的优势，满足实际应用需求。

a 原始图像



b QR 码水印图像

c 文本水印图像

图 9　实验数据
Fig.9 Experimental Data

表 6　算法对比实验结果
Tab.6 Experimental results of algorithm contrast

算法	嵌入水印信息位数/bit	水印容量(字数)	缩放因子					
			0.25	0.5	1.0	1.5	2	10
文献[14]算法	4356	20	提取失败	实验数据为XX省XX大学XX学院所有使用期间禁	实验数据为XX省XX大学XX学院所有使用期间禁	实验数据为XX省XX大学XX学院所有使用期间禁	提取失败	提取失败
文献[16]算法	4356	20	提取失败	实验数据为XX省XX大学XX学院所有使用期间禁	实验数据为XX省XX大学XX学院所有使用期间禁	实验数据为XX省XX大学XX学院所有使用期间禁	实验数据为XX省XX大学XX学院所有使用期间禁	提取失败
文中算法	128	31						

4　结语

文中基于 QR 码预处理和圆形角度模板提出了一种抗缩放攻击的高水印容量数字水印算法，该算法具备以下特点：根据 QR 码生成原理，提取 QR 码的数据编码信息以压缩待嵌入水印信息量，之后通过角度编码提高水印容量；摒弃常见以 0/1 二值序列嵌入水印的思想，通过构建具有角度信息的圆形模板实现水印的嵌入，提升了水印信息的稳健性；水印信息检测不再是水印嵌入的逆过程，而是通过检测圆形角度模板中包含的角度特征信息而得到水印信息，提高了算法的鲁棒性。

综上所述，文中算法不仅提升了水印信息容量，而且可抵抗高强度的缩放攻击，以及其他（色彩调整、旋转、压缩、噪声等）图像处理攻击，对图像的安全保护具有一定的应用价值。在未来的研究中，可通过构建特征水印，使得该算法迅速定位水印起始位置，在满足上述抗攻击能力的基础上，实现抗裁剪攻击。

参考文献：

[1] 朱长青, 许德合, 任娜, 等. 地理空间数据数字水印理论与方法[M]. 第 1 版. 北京: 科学出版社, 2014:7.
ZHU Chang-qing, XU De-he, REN Na, et al. Digital Watermarking Theory and Method for Geospatial Data[M]. The First Edition. Beijing: Science Press, 2014: 7.

[2] 何冰. 基于 LSB 的抗旋转攻击鲁棒性数字水印算法[J]. 系统仿真技术, 2010, 6(4): 304—307.
HE Bing. A Digital Image Watermarking Method Against Rotation Attack Based on LSB[J]. System Simulation Technology, 2010, 6(4): 304—307.

[3] KURDI M M, ELZEIN I A, ZEKI A M. Least Significant Bit (LSB) and Random Right Circular Shift (RRCF) in Digital Watermarking[C]// Computer Engineering Conference. IEEE, 2017.

[4] 邢丹, 王雷, 乔玉. 一种基于图像统计特性的空域水印算法[J]. 电子技术与软件工程, 2015(8): 102.
XING Dan, WANG Lei, QIAO Yu. A Spatial Domain Watermarking Algorithm Based on Image Statistics[J]. Electronic Technology & Software Engineering, 2015(8): 102.

[5] 朱长青. 一种基于伪随机序列和 DCT 的遥感影像水印算法[J]. 武汉大学学报(信息科学版), 2011, 36(12): 1427—1429.
ZHU Chang-qing. An Algorithm for Digital Watermark Based on Pseudo-Random Sequence and DCT for Remote Sensing Image[J]. Geomatics and Information Science of Wuhan University, 2011, 36(12): 1427—1429.

[6] LIU L Y. Research and Implement of Digital Image Watermark Based on DCT[J]. Advanced Materials Research, 2014, 3326(989): 4086—4090.

[7] CHEN A, WANG X. An Image Watermarking Scheme Based on DWT and DFT[C]// International Conference on Multimedia and Image Processing. IEEE Computer Society, 2017: 177—180.

[8] GUPTA R, MUNDRA P, KARWAL S, et al. DWT-SVD based Watermarking Scheme of JPEG Images Using Elliptic Curve Cryptography[C]// International Conference on Reliability, INFOCOM Technologies and Optimization. IEEE, 2016: 359—365.

[9] 周广州, 陈青, 熊蒙, 等. 一种基于 Harris 特征点和 DWT-SVD 的图像盲水印算法[J]. 包装工程, 2016 , 37(19): 191—194.
ZHOU Guang-zhou, CHEN Qing, XIONG Meng, et al. An Image Watermarking Algorithm Based on Harris Feature Points and DWT-SVD[J]. Packaging Engineering, 2016, 37(19): 191—194.

[10] FAZLI S, MOEINI M. A Robust Image Watermarking Method Based on DWT, DCT, and SVD Using A New Technique for Correction of Main Geometric Attacks[J]. Optik, 2016, 127(2): 964—972.

[11] 陈青, 姚绍华, 陈祥. 基于 SURF 的 NSCT 域抗几何攻击水印算法[J]. 包装工程, 2018, 39(1): 162—167.
CHEN Qing, YAO Shao-hua, CHEN Xiang. NSCT-domain Watermarking Algorithm Robust to Geometric Attacks Based on SURF[J]. Packaging Engineering, 2018, 39(1): 162—167.

[12] 李丽丽, 孙劲光. 基于 Contourlet 变换的遥感影像数字水印方案[J]. 计算机应用与软件, 2012, 29(2): 60—63.
LI Li-li, SUN Jing-guang. A Watermarking Scheme for Remote Sensing Images Based on Contourlet Transformation[J]. Computer Applications and Software, 2012, 29(2): 60—63.

[13] 赵伟光, 尹忠海, 周拥军, 等.基于差分网格的抗 RSD 攻击盲指纹方案[J].计算机应用, 2011, 31(9): 2373—2377.
ZHAO Wei-guang, YIN Zhong-hai, ZHOU Yong-jun, et al. Blind Fingerprint Scheme Against RSD Attacks Based on Differential Grid[J]. Journal of Computer Applications, 2011, 31(9): 2373—2377.

[14] 周拥军, 尹忠海, 高大化. 一种抗缩放攻击的盲检测数字水印方案[J]. 计算机应用, 2010, 30(5): 1233—1235.
ZHOU Yong-jun, YIN Zhong-hai, GAO Da-hua. Blind Digital Watermarking Scheme Against Scaling Attack[J]. Journal of Computer Applications, 2010, 30(5): 1233—1235.

[15] 陈青, 王飞. 基于 SIFT 的 NSCT 域抗几何攻击水印算法[J]. 包装工程, 2017, 38(5): 178—182.
CHEN Qing WANG Fei. NSCT-domain Watermarking Algorithm Robust to Geometric Attacks Based on SIFT[J]. Packaging Engineering, 2017, 38(5): 178—182.

[16] 陈青, 陈祥, 姚绍华. 一种新的 SIFT 几何校正的抗几何攻击水印算法[J]. 包装工程, 2017, 38(1): 169—173.
CHEN Qing, CHEN Xiang, YAO Shao-hua. A New Watermarking Algorithm Against Geometric Attack Based on SIFT Geometric Correction[J]. Packaging Engineering, 2017, 38(1): 169—173.

[17] THULASIDHARAN P P, NAIR M S. QR Code Based Blind Digital Image Watermarking with Attack Detection Code[J]. AEU-International Journal of Electronics and Communications, 2015, 69(7): 1074—1084.

[18] 栾炜, 曹建农. 基于 QR 码和 DWT-SVD 分解的双水印算法[J]. 包装工程, 2018, 39(19): 197—203.
LUAN Wei, CAO Jian-nong. Dual Watermarking Algorithm Based on QR Code and DWT-SVD Decomposition[J]. Packaging Engineering, 2018, 39(19): 197—203.

[19] CHOW Y W, SUSILO W, TONIEN J, et al. A QR Code

Watermarking Approach Based on the DWT-DCT Technique[C]// Information Security and Privacy: 22nd Australasian Conference, 2017: 314—331.

[20] 王潇, 任娜, 朱长青, 等. 基于 QR 码和量化 DCT 的遥感影像数字水印算法[J]. 地理与地理信息科学, 2017, 33(6): 19—24.
WANG Xiao, REN Na, ZHU Chang-qing, et al. A Digital Watermarking Algorithm Based on QR Code and Quantization DCT for Remote Sensing Image[J]. Geography and Geo-Information Science, 2017, 33(6): 19—24.

[21] 林威, 翟信德, 朱长青, 等. 基于 QR 码的遥感影像数字水印算法[J]. 北京邮电大学学报, 2015, 38(1): 26—30.
LIN Wei, ZHAI Xin-de, ZHU Chang-qing. QR Code Based Research on Digital Watermark Algorithm for Remote Sensing Image[J]. Journal of Beijing University of Posts and Telecommunications, 2015, 38(1): 26—30.

[22] GB/T 18284—2000, 快速响应矩阵码[S].
GB/T 18284—2000, Quick Response Code[S].

[23] PRAMILA A, KESKINARKAUS A, TAKALA V, et al. Extracting Watermarks from Printouts Captured with Wide Angles Using Computational Photography[J]. Multimedia Tools & Applications, 2017, 76(15): 16063—16084.

[24] 王潇. 面向屏摄过程的遥感影像数字水印算法研究[D]. 南京: 南京师范大学, 2018.
WANG Xiao. Research on Digital Watermarking Algorithm Oriented to Screen Capture Process for Remote Sensing Image[D]. Nanjing: Nanjing Normal University, 2018.

[25] 李旭东. 抗亮度和对比度攻击的 DCT 域图像数字水印算法[J]. 光电子·激光, 2013, 24(6): 1184—1190.
LI Xu-dong. Image Digital Watermarking Algorithm in DCT Domain for Resisting Brightness-and-contrast Adjusting Attack[J]. Journal of Optoelectronics·Laser, 2013, 24(6): 1184—1190.

[26] 梅靓雅. 基于非采样 Contourlet 变换的第二代遥感影像数字水印算法研究[D]. 南京: 南京师范大学, 2017.
MEI Liang-ya. Research on Second Generation Digital Watermark Algorithm of Remote Sensing Image Based on Nonsubsampled Contourlet Transform[D]. Nanjing: Nanjing Normal University, 2017.